REGIMENTOS E NORMAS

Abril/2026

Política de Segurança da Informação: POSIN

Epagri

SAPE
SECRETARIA DA AGRICULTURA E PECUÁRIA

SAPE
SECRETARIA DA AGRICULTURA E PECUÁRIA

Governador do Estado
Jorginho dos Santos Mello

Secretário de Estado da Agricultura
Admir Edi Dalla Cort

Presidente da Epagri
Dirceu Leite

Diretores

Andréia Meira
Ensino Agrotécnico

Jurandi Teodoro Gugel
Desenvolvimento Institucional

Fabrícia Hoffmann Maria
Administração e Finanças

Gustavo Gimi Santos Claudino
Extensão Rural e Pesqueira

Reney Dorow
Ciência, Tecnologia e Inovação

Epagri

Abril/2026

REGIMENTOS E NORMAS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – POSIN

Aprovado em reunião da Diretoria Executiva em 12/01/2026

Empresa de Pesquisa Agropecuária e Extensão Rural de Santa Catarina.
Florianópolis
2026

Empresa de Pesquisa Agropecuária e Extensão Rural de Santa Catarina (Epagri)
Rodovia Admar Gonzaga, 1.347, Itacorubi, Caixa Postal 502
88034-901, Florianópolis, Santa Catarina, Brasil Fone: (48) 3665-5000
Site: www.epagri.sc.gov.br

Editado pelo Departamento Estadual de Marketing e Comunicação (DEMC/Epagri)
Grupo de Trabalho: Carlos Magno dos Santos Júnior (Gerente do DJUR), Denilson Dortzbach (Gerente do DEPLAN), Eduardo Martins Carvalho (DEGTI), José Pedro Rosses (Controlador Interno e Ouvidor), Eduardo Nathan Antunes (CIRAM), Renato Deggau (DEGTI), Roseleine C. de Mello (DEGTI), Sandro da Silva dos Santos (DEGP), Natália Junqueira Carvalho Costa (DPO - Encarregada de Dados da Epagri), Angela Medeiros Viana Carvalho (DPO - ex-encarregada de dados da Epagri)
Editoração técnica: Paulo Sergio Tagliari
Revisão textual: Laertes Rebelo, Maria Luíza Chaves
Diagramação: Victor Berretta
Distribuição: *on-line*
Primeira edição: Abril de 2026

É permitida a reprodução parcial deste trabalho desde que a fonte seja citada.

Ficha catalográfica

S231p Santa Catarina. Empresa de Pesquisa Agropecuária e Extensão Rural de Santa Catarina.
Política de Segurança da Informação: POSIN. – Florianópolis : Epagri, 2026.
81 p. ; – (Regimentos e Normas).

1. Segurança da informação. 2. Acesso à informação. 3. Gestão de riscos. 4. Privacidade e Proteção de dados. 5. Epagri. I. Título.

CDD: 005.8

Elaborado por: Bibliotecária Rafaela Rocha Rabelo CRB-14/1934

APRESENTAÇÃO

A Política de Segurança da Informação da Epagri (POSIN) estabelece as diretrizes, normas e responsabilidades fundamentais para a proteção dos ativos de informação da Empresa. Este documento fundamenta-se na Lei Geral de Proteção de Dados Pessoais (LGPD) e nas diretrizes de governança do Estado de Santa Catarina, como o Decreto nº 1.184, de 1º de março de 2021, consolidando o compromisso da Epagri com a segurança institucional e a transparência de seus processos.

Trata-se de um instrumento normativo essencial com o objetivo central de mitigar riscos e garantir a confidencialidade, integridade e disponibilidade dos dados institucionais. A POSIN norteia a conduta de todos os colaboradores, contratados, parceiros e terceiros que acessem ou processem informações sob custódia da Epagri.

Aprovada pela Diretoria Executiva em 12/01/2026 (SGPe 865/2021), esta política reflete a situação atual da Epagri e será revisada periodicamente para acompanhar a evolução tecnológica. Sua aplicação permite que as unidades organizacionais estabeleçam relações seguras de troca de dados, garantindo que a informação — um dos bens mais valiosos da Empresa — seja gerida com o máximo rigor, responsabilidade e conformidade legal.

A Diretoria Executiva

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas
ANPD – Agência Nacional de Proteção de Dados
BIA – Análise de Impacto nos Negócios (*Business Impact Analysis*)
CGE – Controladoria-Geral do Estado
CIAI – Comissão Interna de Acesso à Informação
CIRAM – Centro de Informações de Recursos Ambientais e de Hidrometeorologia de Santa Catarina
CMAI – Comissão Mista de Acesso à Informação
CPAD – Comissão Permanente de Avaliação de Documentos
CTEC – Câmara Técnica Consultiva
DEGP – Departamento Estadual de Gestão de Pessoas
DEGOP – Departamento Estadual de Gestão Operacional
DEPLAN – Departamento Estadual de Planejamento e Estratégia
DEGTI – Departamento Estadual de Gestão da Tecnologia da Informação
DEMC – Departamento Estadual de Marketing e Comunicação
DJUR – Departamento Jurídico
DPO – Encarregado de Dados (*Data Protection Officer*)
E-SIC – Serviço de Informações ao Cidadão (meio eletrônico)
GGG – Grupo Gestor do Governo
IA – Inteligência Artificial
IEC – Comissão Eletrotécnica Internacional (*International Electrotechnical Commission*)
ISO – Organização Internacional para Padronização (*International Organization for Standardization*)
LAI – Lei de Acesso à Informação (Lei Federal nº 12.527/2011)
LGPD – Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709/2018)
LLM – Modelo de Linguagem de Grande Escala (*Large Language Models*)
LMS – Sistema de Gestão de Aprendizagem (*Learning Management System*)
MFA – Autenticação de Multifatores (*Multifactor Authentication*)
NBR – Norma Brasileira Regulamentadora
PCD – Plano de Classificação de Documentos
PCN – Plano de Continuidade de Negócios
PGRSI – Plano de Gestão de Riscos de Segurança da Informação
POSIN – Política de Segurança da Informação

SGP-e – Sistema de Gestão de Processos Eletrônicos
SIC – Serviço de Informações ao Cidadão
SSO – Login Único (*Single Sign On*)
TCI – Termo de Classificação de Informação
TTD – Tabela de Temporalidade de Documentos
VPN – Rede Virtual Privada (*Virtual Private Network*)

Sumário

1 DISPOSIÇÕES PRELIMINARES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – POSIN

No Estado de Santa Catarina, a Política de Segurança da Informação (POSIN) foi regulamentada pela Instrução Normativa SEA nº 20/2021.

Na Epagri, a Política de Segurança da Informação tem como **objetivo** estabelecer os princípios, as diretrizes, as responsabilidades, as competências, os subsídios e as práticas para a proteção das informações. Ela visa garantir a confidencialidade, a integridade e a disponibilidade das informações, assegurando o seu uso adequado, a mitigação de riscos à segurança da informação, o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e de outras normas vigentes.

Esta Política se aplica a todos os ativos de informação da Epagri, incluindo dados, sistemas, aplicativos, dispositivos e redes, sejam em instalações físicas ou digitais administradas ou custodiadas pela Epagri. Ela abrange, também, todos os colaboradores, funcionários, contratados, parceiros e terceiros que acessam ou processam as informações da Epagri.

Esta Política está de acordo com a missão, a visão e os valores da Epagri.

Em cumprimento às diretrizes do Estado, a POSIN está integrada por oito planos.

1.1 Plano de Continuidade de Negócios (PCN)

O Plano de Continuidade de Negócios (PCN) visa estabelecer diretrizes e estratégias para assegurar a resiliência operacional da Epagri frente a eventos disruptivos, garantindo a manutenção ou a rápida retomada dos serviços essenciais e estratégicos, como as atividades de pesquisa, extensão rural e ensino agrotécnico. Seu objetivo é minimizar o impacto de interrupções, protegendo a infraestrutura, os sistemas de informação e os dados críticos. O PCN se estrutura a partir da Análise de Impacto nos Negócios (BIA) para priorizar funções, estabelecendo Planos de Contingência para setores críticos e definindo protocolos de comunicação em situações de crise, observando riscos como falhas tecnológicas, desastres naturais e problemas logísticos.

1.2 Plano de Gestão de Ativos de Informação

Este Plano define os processos e procedimentos para a gestão do ciclo de vida dos ativos de informação (dados, sistemas, equipamentos), desde a aquisição até o

descarte, garantindo sua segurança, confidencialidade, disponibilidade e integridade. Seu objetivo é identificar e proteger os ativos essenciais para a Epagri, assegurando a conformidade com a LGPD e a Lei de Acesso à Informação (LAI). As diretrizes incluem manter um Inventário de Ativos detalhado com requisitos de segurança e base legal para dados pessoais e promover a classificação da informação (pública, pessoal ou sigilosa), sendo que a publicidade é a regra geral e o sigilo, a exceção.

1.3 Plano de Gestão de Riscos de Segurança da Informação (PGRSI)

O Plano estabelece os processos para identificar, analisar, avaliar e tratar riscos nos sistemas e processos da Epagri, buscando a segurança, confidencialidade, integridade e disponibilidade das informações. O objetivo é reduzir vulnerabilidades e assegurar a continuidade dos serviços, alinhando-se a boas práticas, como a ABNT NBR ISO/IEC 27005 e o Modelo das Três Linhas. O processo de gestão de riscos é contínuo, compreendendo as etapas de identificação, análise, avaliação e tratamento dos riscos de segurança da informação, com registro em uma matriz de riscos para priorização e estabelecimento de planos de ação.

1.4 Plano de Gestão de Contratos

O Plano de Gestão de Contratos define medidas para garantir que as contratações e parcerias com terceiros estejam em conformidade com a LGPD, assegurando o uso correto de dados pessoais e mitigando riscos de vazamento. Seu principal foco é a obrigatoriedade de incluir cláusula específica sobre proteção de dados e LGPD em novos contratos e a revisão de contratos vigentes, estabelecendo regras claras sobre o objeto, a finalidade, a base legal e as medidas de segurança a serem adotadas pelos contratados e parceiros da Epagri. O Plano ainda estabelece o protocolo para a comunicação obrigatória de incidentes de segurança pelos contratados e parceiros à Epagri.

1.5 Plano de Controle de Acesso à Informação

Este Plano estabelece processos para o controle de acesso às informações custodiadas pela Epagri, visando prevenir acessos não autorizados que possam resultar em tratamento inadequado ou ilícito dos dados. O controle abrange tanto o acesso lógico

(sistemas e redes) quanto o acesso físico (ambientes e equipamentos). As diretrizes centrais são a gestão centralizada das contas de acesso com uso de autenticação de multifatores (MFA) para acesso remoto e contas administrativas e a restrição de acesso aos sistemas que tratam dados pessoais ao mínimo necessário, em conformidade com os princípios da LGPD.

1.6 Plano de Consentimento de Dados

O Plano de Consentimento de Dados estabelece diretrizes para a obtenção, registro e gestão do consentimento aplicáveis às situações em que o tratamento de dados não se enquadra nas demais bases legais da LGPD (ex: execução de políticas públicas). O objetivo é assegurar que o consentimento seja sempre claro, livre, informado e específico (sendo nulas as autorizações genéricas). O Plano define casos de uso (como eventos não vinculados a políticas públicas e publicações com dados não anonimizados) e estabelece que o consentimento deve ser registrado por escrito ou outro meio inequívoco, sendo o processo de revogação gratuito e facilitado ao titular.

1.7 Plano de Proteção de Dados Pessoais baseado na LGPD

Este Plano estabelece diretrizes e procedimentos para o tratamento seguro e adequado de dados pessoais, buscando salvaguardar dados pessoais e sensíveis e prevenir o uso indevido, vazamentos ou acessos não autorizados. O Plano foca em garantir o tratamento com base legal adequada, finalidade legítima e transparência. As diretrizes incluem a manutenção de um inventário atualizado de dados pessoais (com finalidade, base legal e tempo de retenção), o registro de todas as atividades no SGP-e para rastreabilidade e o estabelecimento de critérios rigorosos para o compartilhamento com terceiros (exigindo base legal e parecer do DPO). O Plano também aborda as diretrizes para o uso responsável de Inteligência Artificial (IA) e LLMs, priorizando a não utilização de dados pessoais sem base legal adequada.

1.8 Plano de Treinamento e Conscientização dos Usuários sobre Segurança da Informação

Este Plano visa garantir que todos os usuários compreendam e apliquem boas práticas de segurança da informação, promovendo uma cultura organizacional voltada

à proteção de dados e à prevenção de incidentes. O objetivo é capacitar continuamente os usuários sobre as regras da POSIN e da LGPD, especialmente sobre a importância da proteção de dados pessoais e sensíveis. O Plano utiliza diversos métodos, incluindo a produção de conteúdo multimídia (como o "Minuto Proteção de Dados Pessoais"), plataformas de e-learning e treinamentos direcionados para setores que lidam com grande volume de dados sensíveis.

- O detalhamento e regras específicas de cada Plano estão nos anexos:
- Anexo I - Plano de Continuidade de Negócios (PCN);
- Anexo II - Plano de Gestão de Ativos de Informação;
- Anexo III - Plano de Gestão de Riscos de Segurança da Informação;
- Anexo IV - Plano de Gestão de Contratos;
- Anexo V - Plano de Controle de Acesso à Informação;
- Anexo VI - Plano de Consentimento de Dados;
- Anexo VII - Plano de Proteção de Dados Pessoais baseado na LGPD;
- Anexo VIII - Plano de Treinamento e Conscientização dos Usuários sobre Segurança da Informação.

2 ANEXO I - PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

2.1 Apresentação

O Plano de Continuidade de Negócios (PCN) visa estabelecer diretrizes, responsabilidades e competências para assegurar a resiliência da Epagri diante de eventos disruptivos que possam interromper suas atividades essenciais e estratégicas, garantindo a manutenção ou rápida retomada dos serviços críticos.

2.2 Objetivos

● O PCN tem como objetivo principal assegurar a resiliência da estatal, minimizando os impactos de interrupções nas operações. Seus objetivos específicos incluem:

● Estabelecer ações e estratégias para manter ou restabelecer os processos essenciais da Epagri em caso de interrupções;

● Minimizar os impactos de eventos disruptivos nas atividades de pesquisa, extensão rural e ensino agrotécnico;

● Definir responsabilidades e fluxos de comunicação em situações de crise;

● Proteger os ativos críticos da Epagri, como infraestrutura, sistemas de informação e recursos humanos;

● Assegurar a confiança dos cidadãos e demais partes interessadas na capacidade da Epagri de manter seus compromissos.

2.3 Campo de Aplicação

Este Plano aplica-se a todas as unidades da Epagri, abrangendo processos e infraestruturas físicas e digitais relacionados à pesquisa agropecuária, extensão rural, ensino agrotécnico, gestão de dados e sistemas, logística, comunicação e manutenção da infraestrutura. O PCN contempla tanto atividades administrativas quanto finalísticas da Epagri.

2.4 Legislação e Boas Práticas

● Lei federal nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

● Lei federal nº 12.527, de 2011 (Lei de Acesso à Informação – LAI);

● Resolução CD/ANPD nº 18, de 2024 (Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais);

● Decreto estadual nº 1.892, de 2022 (atribuições e requisitos da função de

encarregado pelo tratamento de dados pessoais);

- Instrução Normativa SEA nº 20, de 2021 (Política de Segurança da Informação – POSIN);
- ABNT NBR 22301 (Segurança e resiliência — Sistema de gestão de continuidade de negócios — Requisitos);
- Política de Porta-Vozes da Epagri.

2.5 Diretrizes

2.5.1 Processos cobertos pelo PCN

- Manutenção das atividades de pesquisa agropecuária, extensão rural e ensino agrotécnico, bem como atividades administrativas;
- Proteção dos sistemas de informação e comunicação;
- Salvaguarda da infraestrutura crítica (laboratórios, centros de pesquisa e redes de atendimento).

2.5.2 Limitações consideradas

- Recursos financeiros: orçamento limitado para investimentos em tecnologias de contingência;
- Capacidade de resposta: dependência de terceiros para suporte técnico/logístico;
- Capacitação: necessidade de treinamento contínuo;
- Localização: dispersão geográfica das unidades.

2.5.3 Estratégias e Estrutura do PCN

- **Análise de Impacto nos Negócios (BIA):** A Diretoria Executiva e o DEPLAN, com o auxílio técnico do Comitê de *Compliance* e, caso necessário, de outras unidades, deverão identificar e priorizar as funções críticas e os impactos de sua interrupção;
- **Planos de contingência para setores críticos:** A partir do levantamento dessas funções críticas, a Diretoria Executiva e o DEPLAN, com o auxílio técnico do Comitê de *Compliance* e, caso necessário, outras unidades, deverá estabelecer um plano de contingência definindo os procedimentos necessários para retomar as operações críticas que afetem a continuidade dos negócios da Epagri. Os planos de contingência devem definir os papéis e responsabilidades das pessoas e unidades envolvidas, prazos e soluções alternativas para a continuidade dos negócios da Epagri ou processos de evacuação;
- **Comunicação em situações de crise:** Para a comunicação em crises, a Diretoria Executiva contará com o apoio do Departamento Estadual de Marketing e Comunicação

para coordenação e informação às partes interessadas, respeitada a Política de Porta-Vozes da Epagri.

2.5.4 Riscos

Para a elaboração dos planos de contingência, devem ser observados riscos críticos para a Epagri, tendo como base o Plano de Gestão de Riscos de Segurança da Informação, o documento Boas Práticas de Controle Interno, Gestão de Riscos e *Compliance* e os riscos previamente identificados no quadro abaixo:

Quadro 1. Lista de Riscos

Categoria de Risco	Risco	Exemplos	Ações
Operacional	Desastres naturais	Enchentes, tempestades, incêndios	Prevenção com infraestrutura adequada, parcerias com a Defesa Civil, realocação temporária e adoção de procedimentos para contratações emergenciais
Operacional	Falhas tecnológicas	Ataques cibernéticos, falhas de servidores	*Backup* regular, suporte técnico, comunicação tempestiva do incidente à ANPD
Operacional	Crises sanitárias	Epidemias e pandemias	Protocolos de saúde, trabalho remoto, reestruturação operacional
Operacional	Problemas logísticos	Falta de insumos ou transporte	Estoques estratégicos, rotas alternativas, novas contratações de fornecedores
Operacional	Quedas de energia	Interrupções prolongadas	Geradores, priorização de equipamentos essenciais, contato com concessionárias
Operacional	Furtos, roubos e extravio de bens	Roubo, extravio ou furtos de computadores e equipamentos com dados pessoais ou de documentos físicos	Manutenção da contratação de serviços de vigilância patrimonial, instalação de câmeras em áreas estratégicas, etc., comunicação tempestiva do incidente à ANPD

2.6 Atribuições e Responsabilidades

2.6.1 Diretoria Executiva

● Aprovar e assegurar recursos para implantação e manutenção deste Plano.

2.6.2 Encarregado de Dados

● Elaborar, revisar e monitorar a execução deste Plano;

● Zelar pelo cumprimento das diretrizes relativas à proteção de dados pessoais durante situações adversas.

2.6.3 Gestores de Unidades

● Implementar o Plano em suas áreas e promover o cumprimento das diretrizes.

2.6.4 Departamento Estadual de Gestão da Tecnologia da Informação (DEGTI)

● Implementar soluções tecnológicas de contingência;
● Monitorar e atualizar os sistemas críticos para garantir a continuidade;
● Realizar testes regulares do PCN;
● Garantir a segurança e a continuidade dos sistemas da Epagri.

2.6.5 Departamento Estadual de Marketing e Comunicação (DEMC)

● Apoiar, coordenar e executar atividades de editoração técnica com fins institucionais, informativos ou educativos, relacionadas ao respectivo Plano;

● Produzir e editar conteúdo jornalístico relacionado à divulgação do respectivo Plano;

● Apoiar a Diretoria Executiva e coordenar a comunicação em crises, respeitada a Política de Porta-Vozes da Epagri.

2.6.6 Usuários

● Seguir as orientações do Plano e participar de treinamentos sobre proteção de dados pessoais;

● Comunicar às autoridades superiores incidentes que possam afetar a continuidade das operações.

2.7 Disposições finais

● O PCN será atualizado periodicamente, especialmente após mudanças organizacionais ou ocorrência de incidentes relevantes;

● As ações descritas neste Plano visam preservar a missão institucional da Epagri e proteger seus ativos essenciais diante de qualquer cenário de interrupção.

3 ANEXO II - PLANO DE GESTÃO DE ATIVOS DE INFORMAÇÃO

3.1 Apresentação

A Epagri lida com ativos de informação que incluem dados confidenciais e públicos essenciais para a prestação de seus serviços e o cumprimento de suas funções. A gestão desses ativos é fundamental para assegurar a continuidade das operações e a proteção dos dados pessoais, conforme a Lei federal nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

Este Plano define os processos e procedimentos para a gestão do ciclo de vida dos ativos de informação, garantindo a sua segurança, confidencialidade, disponibilidade, autenticidade, integridade e transparência.

3.2 Objetivos

Os objetivos deste Plano são:

- Definir diretrizes para a identificação e proteção dos ativos de informação.
- Assegurar a gestão do ciclo de vida dos ativos de informação, desde a sua aquisição até o descarte;
- Estabelecer responsabilidades para a gestão de ativos de informação, alinhadas às boas práticas e às legislações aplicáveis;
- Garantir a conformidade com a LGPD e outras normas de proteção de dados e de segurança da informação.

3.3 Campo de aplicação

Este Plano aplica-se a:

- Todos os usuários e unidades da Epagri.

3.4 Legislação e Boas Práticas

- Lei federal nº 13.709 de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- Lei federal nº 12.527, de 2011 (Lei de Acesso à Informação – LAI);

- Resolução CD/ANPD nº 18, de 2024 (Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais);
- Decreto estadual nº 1.048, de 2012 (regulamenta a LAI no âmbito estadual);
- Decreto estadual nº 1.892, de 2022 (atribuições e requisitos da função de encarregado pelo tratamento de dados pessoais);
- Instrução Normativa SEA nº 20, de 2021 (Política de Segurança da Informação – POSIN);
- Instrução Normativa SEA nº 10, de 2024 (Procedimentos para a eliminação de documentos públicos e seleção de amostras).

3.5 Diretrizes Gerais

3.5.1 Gestão do Ciclo de Vida dos Ativos de Informação

- **Planejamento:** identificação das necessidades de ativos de informação e alinhamento com os objetivos estratégicos da Epagri, incluindo a revisão dos ativos de informação existentes e análise de custo-benefício de compra e instalação de novos ativos de informação;
- **Aquisição:** definição de requisitos técnicos e regras contratuais na aquisição de ativos de informação, em conformidade com a Lei federal nº 13.303/2016 (Lei das Estatais), Regulamento Interno de Licitações e Contratos (RILC-Epagri) e demais normas internas e externas de aquisições.
- **Implantação:** instalação e configuração dos ativos de informação, garantindo que estejam operacionais conforme os padrões estabelecidos;
- **Gerenciamento:** controle contínuo, incluindo manutenção, atualização e monitoramento dos ativos de informação para garantir sua integridade e disponibilidade;
- **Descarte:** processo seguro de desativação ou eliminação dos ativos de informação que não são mais necessários, garantindo a remoção de dados confidenciais em conformidade com a Instrução Normativa SEA nº 10/2024 e as diretrizes da Comissão Permanente de Avaliação de Documentos (CPAD).

3.5.2 Inventário de Ativos de Informação

- O inventário de ativos de informação deve incluir informações sobre os responsáveis por eles, requisitos de segurança, interdependências entre os ativos e, no caso de dados pessoais, a finalidade, a necessidade e a base legal para o seu tratamento;

● O DEGTI deve utilizar ferramentas de descoberta de ativos de informação e inventário automatizado sempre que possível para garantir que todos os ativos de informação estejam devidamente registrados e atualizados.

3.5.3 Identificação e Proteção de Ativos de Informação

● Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela Epagri é considerada ativo de informação e faz parte do seu patrimônio, devendo ser protegida, observadas a LGPD e a LAI;

● Todos os ativos de informação devem ser identificados e classificados de acordo com seu nível de confidencialidade (público, pessoal ou sigiloso);

● Informações sigilosas devem ser classificadas e protegidas conforme a legislação vigente, incluindo a LAI e regulamentos estaduais;

● O acesso a informações confidenciais deve ser restrito a usuários autorizados, em conformidade com o **Plano de Controle de Acesso à Informação da POSIN.**

3.5.4 Acesso à Informação e Comissão Interna de Acesso à Informação (CIAI)

• **A publicidade será preceito geral e o sigilo exceção**, conforme as diretrizes do art. 3º da LAI. Todos têm direito de receber da Epagri informações de seu interesse particular, de interesse coletivo ou geral, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

• A Epagri divulgará informações de interesse público, independentemente de solicitações, no seu Portal da Transparência ou em outros meios, ou ainda mediante pedido de acesso à informação encaminhado à Ouvidoria, por meio do Serviço de Informações ao Cidadão (e-SIC): https://www.epagri.sc.gov.br/index.php/e-sic/

• A Comissão Interna de Acesso à Informação (CIAI), composta por 3 (três) empregados públicos efetivos, nomeada por portaria do Diretor-Presidente da Epagri, coordenará, **exclusivamente**, a classificação das informações sigilosas listadas no art. 23 da LAI e art. 27 do Decreto estadual nº 1.048, de 2012.

● Informações protegidas por outro tipo de sigilo legal (sigilo fiscal, bancário, de operações e serviços no mercado de capitais, comercial, profissional, industrial, segredo de justiça, dados pessoais sensíveis), não listadas nos artigos acima, **não devem ser classificadas pela CIAI** e devem ter o seu acesso restrito e seu sigilo resguardado, na forma da legislação.

3.5.5 Descarte e atuação da Comissão Permanente de Avaliação de Documentos (CPAD)

• A Comissão Permanente de Avaliação de Documentos (CPAD) é o órgão responsável por analisar, classificar e determinar a destinação dos documentos produzidos e recebidos pela Epagri. Sua atuação assegura a preservação de informações relevantes e a eliminação segura de documentos desprovidos de valor administrativo, fiscal ou histórico, garantindo que a documentação essencial seja corretamente arquivada e acessível, o que fomenta a transparência e a eficiência administrativa. Sua organização está estabelecida na Instrução Normativa SEA nº 8/2024;

• A Epagri deve classificar e organizar os conjuntos documentais em conformidade com os instrumentos de gestão documental publicados no âmbito da Administração Pública Estadual: o Plano de Classificação de Documentos (PCD) e a Tabela de Temporalidade de Documentos (TTD) para atividades-meio, conforme a Instrução Normativa SEA nº 4/2025;

• A Epagri adota as diretrizes da Tabela de Temporalidade da SEA/SC para as atividades-meio. A Tabela de Temporalidade da Epagri contemplará a descrição dos documentos produzidos pela Empresa, abrangendo as áreas-meio e a área-fim (extensão rural e pesqueira, pesquisa e ensino profissional agrotécnico);

• Caso haja falta de previsão de algum tipo documental no PCD ou TTD (atividades-meio ou finalísticas), a área produtora dos documentos deverá solicitar à CPAD a sua inclusão nos referidos instrumentos, visando à classificação e avaliação da destinação;

• A CPAD orientará as unidades administrativas da Epagri na classificação dos documentos e na aplicação da tabela de temporalidade. Isso inclui a seleção dos documentos passíveis de eliminação e de suas respectivas amostras, sempre sob orientação e acompanhamento, quando necessário, da Gerência de Gestão Documental (GEDOC);

• À GEDOC compete normatizar, supervisionar, fiscalizar e orientar tecnicamente os órgãos setoriais e seccionais quanto aos procedimentos administrativos de eliminação de documentos públicos, conforme os instrumentos de gestão documental publicados e demais normas vigentes;

• Conforme estabelece a Instrução Normativa SEA nº 05/2024, os documentos produzidos até **31 de dezembro de 1985** ou aqueles sob custódia do Estado nesta data, provisoriamente não poderão ser eliminados. A listagem de eliminação referente a esse período deverá ser encaminhada à GEDOC para avaliação e posterior submissão à Câmara Técnica Consultiva (CTEC);

• A eliminação de documentos públicos em suporte físico não exige a digitalização prévia. A digitalização deve ser realizada apenas mediante justificativa clara, necessidade comprovada e se os prazos de guarda estiverem em curso;

• Os documentos públicos em suporte físico, cuja destinação não for a guarda permanente, poderão ser substituídos por representantes digitais. Os originais físicos poderão ser eliminados após o processo de digitalização, desde que cumpridos os procedimentos previstos pela Instrução Normativa SEA nº 07/2021 ou outra que venha a substituí-la;

• Após a digitalização, os documentos digitais deverão seguir o processo de destinação estabelecido nas TTDs (atividades-meio e atividades-fim), que preveem a preservação até o esgotamento dos prazos de guarda corrente e intermediária;

• A eliminação de documentos públicos da Epagri ocorrerá após a conclusão do processo de avaliação e seleção da documentação, que serão realizados pelas unidades produtoras e custodiadoras e conduzidos pelas respectivas Subcomissões Permanentes de Avaliação de Documentos (CPADs). A eliminação será efetivada quando cumpridos os procedimentos estabelecidos na Instrução Normativa SEA nº 10/2024;

• O documento poderá ser eliminado na Epagri após cumprir os períodos mínimos de guarda corrente e intermediária, mediante aprovação da CPAD, autorização do GEDOC e lançamento de Edital de Eliminação, observando-se os trâmites da Instrução Normativa SEA nº 10/2024;

• Alternativamente, após cumprir os períodos mínimos de guarda corrente e intermediária, o documento poderá ser recolhido ao Arquivo Público Estadual, que realizará a análise final sobre a guarda permanente ou a eliminação;

● É responsabilidade da Epagri, como controladora dos dados pessoais, detalhar e especificar quais documentos encaminhados ao Arquivo Público Estadual estão protegidos pela Lei Geral de Proteção de Dados (LGPD) e pela Lei de Acesso à Informação (LAI), incluindo o período de sigilo a ser aplicado.

3.6 Atribuições e Responsabilidades

3.6.1 Departamento Estadual de Gestão da Tecnologia da Informação (DEGTI)

● Realizar o mapeamento dos ativos de informação, mantendo registros atualizados;

● Implementar ferramentas para inventário automatizado de ativos físicos e de *software;*

● Monitorar e atualizar o inventário de ativos de informação, incluindo a

configuração de novos ativos de informação e a coordenação da retirada de equipamentos obsoletos;

● Coordenar a desativação e o descarte lógico das informações contidas nos ativos físicos, minimizando riscos de vazamento e subsidiando a possibilidade do descarte pelo DEGOP;

● Garantir que os ativos de *software* estejam sempre atualizados e em conformidade com os padrões de segurança.

3.6.2 Departamento Estadual de Gestão Operacional (DEGOP)

● Providenciar a baixa patrimonial dos ativos físicos inservíveis;

● Após o descarte da informação lógica pelo DEGTI, realizar o descarte dos ativos físicos inservíveis.

3.6.3 Departamento Estadual de Marketing e Comunicação (DEMC)

● Apoiar, coordenar e executar atividades de editoração técnica com fins institucionais, informativos ou educativos, relacionadas ao respectivo Plano;

● Produzir e editar conteúdo jornalístico relacionado à divulgação do respectivo Plano.

3.6.4 Gestores de Unidades da Epagri

● Auxiliar o DEGTI na identificação e atualização dos ativos de informação sob sua responsabilidade;

● Informar ao DEGTI e/ou DEGOP sobre alterações na utilização de ativos de informação, como movimentação de equipamentos entre unidades;

● Assegurar que os usuários sob sua supervisão sigam as políticas de segurança e gestão de ativos de informação e demais orientações do DEGTI, DEGOP e Encarregado de Dados.

3.6.5 Encarregado de Dados

● Garantir que o tratamento de dados pessoais nos ativos de informação mapeados pelo DEGTI esteja em conformidade com a LGPD;

● Elaborar e atualizar o inventário de dados, a partir do mapeamento de processos institucionais em que haja tratamento de dados pessoais, com vistas à identificação do

ciclo de vida dos dados pessoais em tratamento na Epagri, conforme o inciso XI do art. 2º do Decreto estadual nº 1.892, de 2022;

● Realizar revisões periódicas do inventário de dados pessoais e orientar o DEGTI sobre a necessidade de ajustes.

3.6.6 Usuários de Ativos de Informação

● Utilizar os ativos de informação de forma responsável, respeitando as políticas de segurança da Epagri;

● Apenas instalar, remover, modificar, criar, desenvolver e executar programas na rede da Epagri com a prévia autorização do DEGTI;

● Devolver todos os ativos físicos e de *software* quando do término do vínculo com a Epagri (pedido de demissão, encerramento de estágio ou bolsa, etc.);

● Colaborar com os processos de manutenção e atualização dos ativos de informação;

● Reportar incidentes de segurança imediatamente ao Encarregado de Dados, conforme o Plano de Resposta a Incidentes de Segurança.

3.6.7 Controle Interno e Ouvidoria

● Gerenciar o Serviço de Informações ao Cidadão (SIC);

● Restringir o acesso a informações classificadas como sigilosas pela Epagri nas respostas aos pedidos de acesso à informação e manifestações apresentados na Ouvidoria, na forma do Decreto estadual nº 1.048, de 2012, Decreto estadual nº 1.933, de 2022 e suas alterações.

3.6.8 Comissão Interna de Acesso à Informação (CIAI)

● Exercer as atribuições listadas no art. 38 e seguintes do Decreto estadual nº 1.048, de 2012;

● Efetuar a classificação do grau de sigilo de informações listadas no art. 23 da LAI e art. 27 do Decreto estadual nº 1.048, de 2012, por meio de Termo de Classificação de Informação (TCI), encaminhando-a ao Presidente para ratificação;

● Atualizar o inventário de informações sigilosas classificadas periodicamente;

● Divulgar no Portal da Transparência da Epagri o rol anual de informações classificadas ou desclassificadas como sigilosas, em cada grau de sigilo, bem como os respectivos TCIs;

● Encaminhar à Ouvidoria o rol anual das informações classificadas/desclassificadas em cada grau de sigilo até 1º de fevereiro do ano subsequente.

3.6.9 Diretor-Presidente

● Ratificar a classificação do grau de sigilo de informações realizada pela CIAI;

● Encaminhar a ratificação dos TCIs à Controladoria-Geral do Estado (CGE), por meio da Chefia de Gabinete ou Secretaria da Diretoria Executiva, no prazo de **30 (trinta) dias** a partir da decisão de ratificação.

3.6.10 Diretoria Executiva

● Aprovar este Plano e suas alterações;

● Assegurar a alocação de recursos necessários para a execução deste Plano.

3.6.11 Comissão Permanente de Avaliação de Documentos (CPAD)

● Exercer as atribuições listadas na Instrução Normativa SEA nº 8/2024 e suas alterações;

● Garantir a criação e aplicação do Plano de Classificação de Documentos (PCD) e a Tabela de Temporalidade de Documentos (TTD) das atividades-meio e atividades finalísticas na Epagri;

● Orientar as unidades administrativas da Epagri a classificar os documentos e a aplicar a tabela de temporalidade, selecionando os documentos passíveis de eliminação e suas respectivas amostras, sob orientação e acompanhamento, sempre que necessário, da Gerência de Gestão Documental (GEDOC);

● Encaminhar à GEDOC listagem com os documentos produzidos até 31 de dezembro de 1985 ou que estavam sob a custódia da Epagri nesta data para posterior envio ao Arquivo Estadual;

● Acompanhar e coordenar a digitalização de documentos públicos quando houver uma justificativa clara, necessidade comprovada e os prazos de guarda em curso e conforme a Instrução Normativa SEA nº 07/2021;

● Coordenar o descarte de documentos físicos após a autorização do GEDOC e lançamento de Edital de Eliminação, conforme regras da Instrução Normativa SEA nº 10/2024 e suas alterações.

3.7 Mapeamento de Ativos de Informação

O processo de mapeamento dos ativos de informação deve considerar os ativos físicos, ativos de *software* e serviços em nuvem.

3.7.1 Inventário e Registro de Ativos de Informação

Deve conter, no mínimo, as seguintes informações, se houver:

- Descrição do ativo de informação;
- Responsáveis (proprietários/custodiantes);
- Data de aquisição;
- Interfaces de cada ativo de informação e as interdependências entre eles;
- Número de série;
- Modelo;
- Fabricante;
- Valor da aquisição;
- Localização;
- Endereço físico (controle de acesso à mídia – MAC), quando aplicável;
- Versão;
- Data de validade da garantia/vida útil;
- Data de descarte/descomissionamento (quando aplicável).

No caso de dados pessoais e dados pessoais sensíveis, o inventário do ativo de informação deve conter:

- Descrição do dado pessoal ou, quando houver, do dado pessoal sensível;
- Finalidade do tratamento dos dados pessoais;
- Base legal para o tratamento (arts. 7º e/ou 11 da LGPD);
- Informações sobre compartilhamento com terceiros (quando houver);
- Fluxo de tratamento dos dados pessoais (como são coletados, retidos/armazenados, processados/usados, compartilhados e eliminados);
- Outras informações, conforme as exigências da Agência Nacional de Proteção de Dados (ANPD), recomendações do Comitê Gestor de Proteção de Dados (CGPD) ou do Encarregado de Dados.

O DEGTI deve revisar e atualizar o inventário sempre que houver novas aquisições e ou descartes.

Informações sobre ativos de informação confidenciais devem ser protegidas e acessadas apenas por pessoal autorizado.

A Epagri deve assegurar que os ativos físicos ou de *software* inventariados possuam contrato de suporte em vigor.

3.7.2 Classificação do Grau de Sigilo de Informações

As informações tratadas pela Epagri podem ter os seguintes níveis de acesso:

Públicas (informações de interesse público), com acesso irrestrito e visível a todos os usuários, inclusive pelo público externo. São todas as informações que não sejam de caráter pessoal ou sigilosas;

Pessoais (dados pessoais e dados pessoais sensíveis), relacionadas à pessoa física identificada ou identificável, que devem ser tratadas na forma da LGPD, LAI e Decreto estadual nº 1.048, de 4 de julho de 2012;

Sigilosas:

● **por procedimento de classificação de sigilo realizado pela CIAI - (art. 23 da LAI e art. 27 do Decreto estadual nº 1.048, de 4 de julho de 2012)**, submetidas temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; ou

● **por expressa determinação legal**, que são informações protegidas por demais hipóteses legais de restrição de acesso, como aquelas submetidas a sigilo fiscal, bancário, comercial, profissional, industrial e segredo de justiça. **Independem de classificação pela CIAI**. Seu fundamento inclui, mas não se limita às seguintes normas:

● **Sigilo fiscal:** protege dados fiscais de contribuintes, como declarações de imposto de renda, cadastros e movimentações tributárias. Lei federal nº 5.172, de 1966 (Código Tributário Nacional) (art. 198);

● **Sigilo industrial e de propriedade intelectual:** protege segredos industriais e informações não divulgadas sobre criações, como pedidos de patente, desenhos industriais, programas de computador, bem como fórmulas, processos, *know-how,* conhecimentos, informações ou dados confidenciais utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto. Lei federal nº 9.279, de 1996 (Lei de Propriedade

Industrial) (arts. 30, 75, 105, 106 e 195), Lei federal nº 9.609, de 1998 (Lei do Programa de Computador) (art. 3º), Lei federal nº 10.603, 2002 (Informação não divulgada) e Lei federal nº 12.529, de 2011 (Lei Antitruste) (art. 86);

● **Sigilo bancário:** protege informações financeiras e bancárias, incluindo saldos, extratos e movimentações financeiras. Lei Complementar federal nº 105, de 2001;

● **Sigilo profissional:** protege informações obtidas por profissionais durante o exercício de suas atividades, como informações médicas, jurídicas e psicológicas de seus clientes e pacientes. Lei federal nº 8.906, de 1994 (advogados); Lei federal nº 12.842, de 2013 (médicos) e demais códigos de ética de cada profissão;

● **Sigilo em pesquisas e criações:** protege informações resultantes de atividades de pesquisa e criação desenvolvidas na Epagri. Lei federal nº 10.973, de 2004 (Lei de Inovação) (art. 12);

● **Segredo de justiça:** restringe o acesso a processos judiciais que envolvem dados relacionados à intimidade, vida privada, honra, imagem ou de interesse da segurança pública, como em ações de família, interesses de crianças e adolescentes e crimes sexuais. Lei federal nº 13.105, de 2015 (Código de Processo Civil) (arts. 11 e 189) e Decreto-Lei nº 3.689, de 1941 (Código de Processo Penal) (art. 201, § 6º);

● **Sigilo em manifestações de Ouvidoria:** protege dados pessoais dos denunciantes e de manifestantes e o teor das denúncias. Lei federal nº 13.460, de 2017 (Lei de Defesa dos Usuários dos Serviços Públicos) (art. 10, § 7º) e Decreto estadual nº 1.933, de 2022.

● **Sigilo de investigações criminais, tomadas de contas especiais e procedimentos correcionais, incluindo sindicâncias e processos administrativos disciplinares:** protege informações desses procedimentos e processos para não comprometer o curso das apurações. Decreto-Lei nº 3.689, de 1941 (Código de Processo Penal) (art. 20) e Instrução Normativa CGE nº 2, de 2021.

● A CIAI, composta por 3 (três) empregados públicos efetivos e nomeada por portaria do Diretor-Presidente, deve classificar **exclusivamente** o grau de sigilo das informações listadas no **rol taxativo** do art. 23 da Lei federal nº 12.527, de 2011 (LAI), e do art. 27 do Decreto estadual nº 1.048, de 2012, conforme as regras e procedimentos dos arts. 38 e seguintes do Decreto estadual nº 1.048, de 2012, e orientações da CGE. Informações que não estejam listadas neste rol taxativo ou com sigilo determinado por outras legislações **não devem** ser classificadas pela CIAI.

● A CIAI deverá encaminhar a classificação formalizada por meio de **Termo de Classificação de Informação (TCI)** para a ratificação do Diretor-Presidente por meio do SGP-e, utilizando o modelo padronizado anexo a este Plano.

● Após a ratificação da classificação pelo Diretor-Presidente, a Chefia de Gabinete

ou a Secretaria da Diretoria Executiva deverá encaminhar o SGP-e dos TCIs à Controladoria-Geral do Estado (CGE), que preside a Comissão Mista de Acesso à Informação (CMAI), no prazo de **30 (trinta) dias**, contados da decisão de ratificação. A CMAI será responsável por manter ou alterar a classificação realizada pela Epagri.

● Classificada a informação como sigilosa e mantida a decisão pela CMAI, a CIAI deverá publicar o TCI das informações classificadas no Portal da Transparência da Epagri (Gestão/A Empresa/Informações Classificadas), em cada grau de sigilo, bem como os respectivos TCIs.

● As informações que forem desclassificadas pela Epagri devem seguir o mesmo procedimento e igualmente devem ser publicadas no Portal da Transparência da Epagri.

● A Ouvidoria deverá negar acesso às informações classificadas como sigilosas, encaminhando na resposta ao requerente a motivação e com a cópia do TCI.

3.8 Disposições finais

Este Plano entra em vigor na data de sua aprovação pela Diretoria Executiva da Epagri e deve ser revisado sempre que houver necessidade para adequação às necessidades da Empresa, adaptação a novas tecnologias, atendimento a requisitos legais e mudanças nos processos internos.

As revisões deste Plano serão conduzidas pelo DEGTI em conjunto com a CIAI, Encarregado de Dados e Controle Interno e Ouvidoria.

Quadro 2. Termo de Classificação de Informação (TCI)

Termo de Classificação de Informação (TCI)	
Órgão ou entidade	Indicar o órgão ou entidade classificadora
Grau de sigilo	Escolher um item
Categoria	Categoria na qual se enquadra a informação
Tipo de documento	Descrição do documento
Data da produção	Data da produção do documento
Dispositivo legal	Indicação de dispositivo legal que fundamenta a classificação
Razões da classificação (deverá ser mantido no mesmo grau de sigilo da informação classificada)	Razões da classificação, observados os critérios estabelecidos no Decreto nº. 1.048/2012
Prazo do sigilo	Indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final
Data da classificação	Data da classificação
Representante da CIAI	Nome/cargo
Representante da CIAI	Nome/cargo
Representante da CIAI	Nome/cargo
Autoridade Ratificadora	Identificação do titular do órgão ou da entidade que ratificou a classificação
Desclassificação em __ / __ / ___ (quando aplicável)	Nome:
	Cargo:
Reclassificação em __ / __ / ___ (quando aplicável)	Nome:
	Cargo:
Redução de Prazo em __ / __ / ___ (quando aplicável)	Nome:
	Cargo:

<table>
<tr><td rowspan="2">Prorrogação de Prazo em
__ / __ / ___ (quando aplicável)</td><td>Nome:
Nome:
Nome:
Nome:
Nome:
Nome:</td></tr>
<tr><td>Cargo:
Cargo:
Cargo:
Cargo:
Cargo:
Cargo:</td></tr>
<tr><td colspan="2">_____
Assinatura do Representante da CIAI

_____
Assinatura do Representante da CIAI

_____
Assinatura do Representante da CIAI</td></tr>
</table>

_____

Assinatura da Autoridade Ratificadora

_____

Assinatura da Autoridade responsável por Desclassificação (quando aplicável)

_____

Assinatura da Autoridade responsável por Reclassificação (quando aplicável)

_____

Assinatura da Autoridade responsável por Redução de Prazo (quando aplicável)

_____

Assinatura das Autoridades responsáveis pela Prorrogação de Prazo (CMAI)
(quando aplicável)

_____

Assinatura das Autoridades responsáveis pela Prorrogação de Prazo (CMAI)
(quando aplicável)

_____

Assinatura das Autoridades responsáveis pela Prorrogação de Prazo (CMAI)
(quando aplicável)

_____

Assinatura das Autoridades responsáveis pela Prorrogação de Prazo (CMAI)
(quando aplicável)

_____

Assinatura das Autoridades responsáveis pela Prorrogação de Prazo (CMAI)
(quando aplicável)

_____

Assinatura das Autoridades responsáveis pela Prorrogação de Prazo (CMAI)
(quando aplicável)

4 ANEXO III - PLANO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

4.1 Apresentação

A tecnologia é essencial para a prestação de serviços pela Epagri, uma vez que, ao processar e transmitir informações públicas e confidenciais, a Empresa deve assegurar a proteção desses dados, em conformidade com a Lei Geral de Proteção de Dados (LGPD).

Este Plano de Gestão de Riscos de Segurança da Informação (PGRSI) estabelece os processos para identificar, analisar, avaliar e tratar riscos nos sistemas e processos da Epagri, buscando a segurança, confidencialidade, disponibilidade, autenticidade, integridade e transparência das informações.

4.2 Objetivo

O objetivo deste Plano é:

- Definir diretrizes, responsabilidades e procedimentos para a gestão de riscos de segurança da informação;
- Reduzir vulnerabilidades;
- Garantir a proteção dos ativos de informação;
- Assegurar a continuidade dos serviços prestados pela Epagri e a proteção dos dados.

4.3 Campo de Aplicação

Este Plano aplica-se:

- Aos sistemas e ativos de informação da Epagri;
- Às unidades da Epagri;
- Aos usuários;
- Aos provedores de serviços em nuvem que armazenam ou processam dados da Empresa.

Quaisquer exceções a este Plano deverão ser documentadas e aprovadas por meio de um processo de gerenciamento de exceções da Epagri.

4.4 Legislação e Boas Práticas

- Lei federal nº 13.709 de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- Resolução CD/ANPD nº 15, de 2024 (Regulamento de comunicação de incidente de segurança);
- Resolução CD/ANPD nº 18, de 2024 (Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais);
- Decreto estadual nº 1.892, de 2022 (Atribuições e requisitos da função de encarregado pelo tratamento de dados pessoais);
- Instrução Normativa SEA nº 20, de 2021 (Política de Segurança da Informação – POSIN);
- Boas Práticas de Controle Interno, Gestão de Riscos e *Compliance*;
- Modelo das Três Linhas do *The Institute of Internal Auditors* (IIA);
- ABNT NBR 16337 (Gerenciamento de riscos em projetos – Princípios e diretrizes gerais);
- ABNT NBR ISO/IEC 27005 (Segurança da informação, segurança cibernética e proteção à privacidade – Orientações para gestão de riscos de segurança da informação);
- ABNT NBR ISO 31000 (Gestão de riscos – Diretrizes);
- ABNT NBR IEC 31010 (Gestão de riscos – Técnicas para o processo de avaliação de riscos).

4.5 Atribuições e Responsabilidades

A gestão de riscos de segurança da informação é um processo contínuo e estruturado, realizado por diversos profissionais, em todos os níveis e unidades da Epagri, orientado para a realização dos objetivos da Empresa e para a proteção de dados. A Epagri adota o modelo das Três Linhas do IIA, que organiza funções em três linhas para garantir uma boa governança e gestão de riscos.

4.5.1 Departamento Estadual de Gestão da Tecnologia da Informação (DEGTI) (1ª linha)

- Conduzir varreduras periódicas de ativos de informação, sistemas e dispositivos para identificar vulnerabilidades;
- Realizar análises de vulnerabilidades em novos sistemas;
- Definir, monitorar e atualizar os níveis de riscos de segurança da informação;

● Definir procedimentos para a análise e revisão periódica de *logs;*

● Coordenar e executar a identificação, a avaliação e o tratamento de riscos, com o auxílio do Comitê de *Compliance*;

● Comunicar vulnerabilidades detectadas ao Comitê de *Compliance* e ao Encarregado de Dados.

4.5.2 Usuários (1ª linha)

● Cumprir as normas e procedimentos de segurança estabelecidos pela Epagri;

● Reportar incidentes de segurança imediatamente ao superior hierárquico e ao Encarregado de Dados, conforme o **Plano de Resposta a Incidentes de Segurança**;

● Participar de treinamentos e ações de conscientização sobre a segurança da informação;

● Reportar ao DEGTI os riscos de segurança na informação presentes em seus processos.

4.5.3 Departamento Estadual de Marketing e Comunicação (DEMC) (1ª linha)

● Apoiar, coordenar e executar atividades de editoração técnica com fins institucionais, informativos ou educativos, relacionadas ao respectivo Plano;

● Produzir e editar conteúdo jornalístico relacionado à divulgação do respectivo Plano.

4.5.4 Encarregado de Dados (2ª linha)

● Orientar e sensibilizar usuários sobre a proteção de dados pessoais;

● Exercer as atribuições previstas no Regimento Interno da Epagri, Decreto estadual nº 1.892, de 2022 e Resolução CD/ANPD nº 18/2024 ou normas supervenientes;

● Apoiar o DEGTI em procedimentos relacionados a incidentes de segurança e vazamento de dados;

● Solicitar apoio aos Usuários, Gestores, Departamento Estadual de Gestão de Pessoas (DEGP), Departamento Estadual de Gestão da Tecnologia da Informação (DEGTI) e Departamento Estadual de Marketing e Comunicação (DEMC), conforme o Plano de Resposta a Incidentes de Segurança da Epagri;

● Monitorar e comunicar incidentes de segurança que possam acarretar risco ou

dano relevante aos titulares de dados pessoais à Agência Nacional de Proteção de Dados (ANPD), na forma da Resolução CD/ANPD nº 15/2024 e do Plano de Resposta a Incidentes de Segurança da Epagri.

4.5.5 Comitê de Conformidade e Gerenciamento de Riscos (Comitê de *Compliance*) (2ª linha)

● Auxiliar o DEGTI na identificação, avaliação e tratamento de riscos, inclusive quanto à metodologia de gestão de riscos a ser utilizada;

● Acompanhar as ações de mitigação de riscos e assegurar a aplicação das boas práticas de controle;

● Avaliar periodicamente a conformidade das medidas implementadas com este Plano e recomendar ajustes.

4.5.6 Auditoria Interna (3ª linha)

● Avaliar, de forma independente, a efetividade, eficiência, eficácia e adequação dos controles e medidas de gestão de riscos adotadas pelas 1ª e 2ª linhas.

4.5.7 Diretoria Executiva (órgão de governança)

● Aprovar este Plano e suas alterações;

● Tomar decisões estratégicas sobre o tratamento de riscos;

● Assegurar que os recursos necessários para a execução deste Plano estejam disponíveis, incluindo eventuais contratações de terceiros e parcerias.

4.6 Processo de Gestão de Riscos de Segurança de Informação

O processo de gestão de riscos de segurança de informação será coordenado pelo DEGTI, com o auxílio do Comitê de *Compliance* e, conforme o caso, dos demais usuários, de acordo com as seguintes etapas:

4.6.1 Identificação de Riscos

● Realizar um mapeamento detalhado dos ativos de informação e identificar riscos associados a cada um;

● Documentar os riscos de segurança da informação identificados em uma matriz de riscos.

4.6.2 Análise e avaliação de Riscos

● Analisar a probabilidade de ocorrência e o impacto de cada risco;

● Classificar o nível de cada risco na matriz de riscos (crítico, alto, médio, baixo, muito baixo);

● Para cada risco identificado e analisado, avaliar se a decisão será evitar, transferir, aceitar ou mitigar o risco.

4.6.3 Tratamento de Riscos (resposta ao Risco)

● Definir medidas de mitigação para os riscos, priorizando a correção das vulnerabilidades, conforme sua criticidade e ameaças;

● Estabelecer um plano de ação para mitigar cada risco identificado, analisado e avaliado (o quê, quem, quanto, quando, como e onde);

● Submeter à Diretoria Executiva as medidas de mitigação de riscos que excedam sua alçada ou que envolvam a necessidade de recursos, para que sejam deliberadas e aprovadas.

4.6.4 Monitoramento, revisão e comunicação

● Implementar as ações de correção, monitorando continuamente o progresso do processo;

● Monitorar continuamente os riscos e avaliar a eficácia das medidas de mitigação, documentando as ações realizadas;

● Realizar revisões periódicas deste Plano e da matriz de riscos;

● Comunicar o Comitê de *Compliance* e a Diretoria Executiva sobre o tratamento de riscos.

A **Figura 1** abaixo resume o processo de Gestão de Riscos

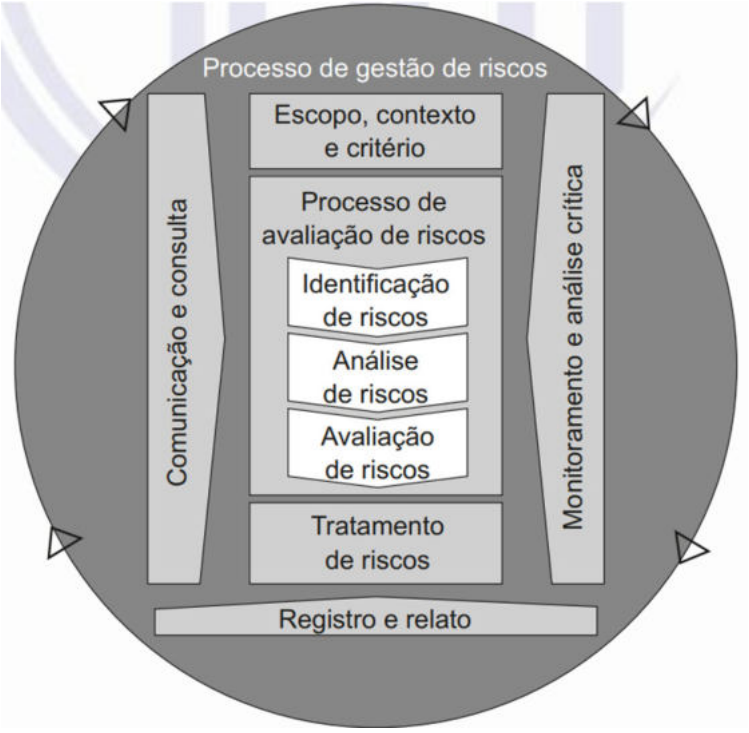

Figura 1. Processo de gestão de riscos
Fonte: ABNT NBR ISO 31000:2018

4.7 Matriz de Riscos e Tratamento de Vulnerabilidades

Para elaborar a matriz de riscos de segurança da informação, o DEGTI poderá se utilizar de várias fontes, como registros de usuários, *sites* de segurança da informação, boletins de segurança ou publicações de fornecedores de *software*, reclamações ou alertas das unidades, entrevistas semiestruturadas e outras técnicas sugeridas na ABNT NBR IEC 31010 e/ou ABNT NBR ISO/IEC 27005. A matriz de riscos deve ser revisada periodicamente e conter informações sobre:

- Instrumento de identificação;
- Fontes;
- Vulnerabilidades;
- Eventos;

● Consequências;

● Análise dos riscos para priorização, conforme sua probabilidade e impacto;

● Plano de ação para a correção ou mitigação dos riscos.

Todo ativo de informação criado, adquirido ou custodiado pela Epagri deverá ser protegido contra ameaças, ataques, incidentes e outras formas de comprometimento à segurança da informação, com o objetivo de minimizar riscos.

4.8 Dos registros de *logs*

O DEGTI deve:

● Identificar eventos a serem registrados em cada sistema e dispositivo;

● Garantir que os *logs* sejam protegidos contra adulteração e acesso não autorizado;

● Realizar análises periódicas dos registros de *logs* para detectar atividades suspeitas;

● Manter os registros pelo tempo necessário para auditorias e investigações.

4.9 Disposições finais

Este Plano entra em vigor na data de sua aprovação pela Diretoria Executiva da Epagri e deve ser revisado sempre que houver necessidade para adequação às necessidades da Empresa, adaptação a novas tecnologias, atendimento a requisitos legais e mudanças nos processos internos.

As revisões deste Plano serão conduzidas pelo DEGTI em conjunto com o Comitê de *Compliance* e Encarregado de Dados.

5 ANEXO IV - PLANO DE GESTÃO DE CONTRATOS

5.1 Apresentação

O plano de gestão de contratos integra a Política de Segurança da Informação (POSIN). Ele define medidas e diretrizes para que as contratações e parcerias realizadas pela Epagri com terceiros estejam em conformidade com a LGPD, assegurando o uso correto de dados pessoais, reduzindo riscos, aumentando a transparência e apoiando gestores na tomada de decisões seguras.

5.2 Objetivos

Os objetivos deste Plano são:

- Assegurar que o tratamento de dados pessoais em contratações e parcerias da Epagri com terceiros esteja em conformidade com a LGPD;
- Definir as regras e procedimentos de segurança para transferência de dados pessoais entre a Epagri, fornecedores, parceiros e outras partes com quem a Empresa se relaciona;
- Proporcionar transparência e respeito aos direitos dos titulares de dados;
- Mitigar riscos de vazamento de dados;
- Estabelecer o protocolo de comunicação obrigatório para a gestão e o reporte de Incidentes de Segurança da Informação;
- Garantir a inclusão de cláusulas contratuais que vinculem a segurança e o tratamento de dados à fiscalização e aplicação de penalidades.

5.3 Campo de Aplicação

Este Plano aplica-se a todos os usuários e unidades da Epagri.

5.4 Legislação e Boas Práticas

- Lei federal nº 13.303, de 2016 (Lei das Estatais);
- Lei federal n º 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- Lei federal nº 12.527, de 2011 (Lei de Acesso à Informação – LAI);
- Resolução CD/ANPD nº 18, de 2024 (Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais);

- Decreto estadual nº 1.048, de 2012 (regulamenta a LAI no âmbito estadual);
- Decreto estadual nº 1.892, de 2022 (atribuições e requisitos da função de encarregado pelo tratamento de dados pessoais);
- Instrução Normativa SEA nº 20, de 2021 (Política de Segurança da Informação – POSIN);
- Regulamento Interno de Licitações e Contratos da Epagri (RILC-Epagri).

5.5 Diretrizes Gerais

5.5.1 Cláusula de proteção de dados e LGPD

Os contratos da Epagri celebrados com terceiros devem conter cláusula específica sobre proteção de dados e LGPD em que constem informações sobre a segurança do tratamento dos dados pessoais, incluindo, mas não se limitando, às seguintes informações:

- Identificação de controlador e operador de dados;
- Conformidade com os princípios legais do art. 6º da LGPD;
- Objeto, duração, natureza, finalidade específica, adequação do tratamento à finalidade e tipos de dados pessoais tratados;
- Medidas de proteção e segurança de dados pessoais, incluindo dados sensíveis e de crianças e adolescentes, conforme o caso;
- Base legal que sustenta o tratamento dos dados pessoais;
- Orientações quanto ao acesso de dados pelos titulares de dados;
- Procedimentos para pedidos de acesso, retificação, bloqueio, restrição, apagamento, portabilidade de dados ou o exercício de quaisquer outros direitos dos titulares de dados;
- Restrições à subcontratação que envolva o tratamento de dados pessoais sem o consentimento prévio e expresso da Epagri.

• Novos contratos devem obrigatoriamente conter cláusula de proteção de dados e LGPD, conforme a legislação vigente e sob orientação do Departamento Jurídico (DJUR).

• Contratos e parcerias que envolvam grande número de compartilhamento de dados pessoais, dados pessoais sensíveis e banco de dados da Epagri, além da cláusula-padrão, devem contar com medidas específicas de proteção e segurança de dados, conforme os riscos envolvidos.

• Contratos e parcerias que estabeleçam o compartilhamento de dados pessoais devem estar de acordo com os art. 11, §§ 3º e 4º, 26, 27, 30 da LGPD e as normas da Agência Nacional de Proteção de Dados (ANPD).

• Contratos e parcerias anteriores a este Plano, firmados após a vigência da LGPD e que não atendam a esta norma, devem ser revisados e, se necessário, a Unidade deve promover termo aditivo para a sua adequação.

5.6 Atribuições e Responsabilidades

5.6.1 Departamento Jurídico

● Elaborar minutas padrão de contratos, incluindo a cláusula de proteção de dados e LGPD, de acordo com as orientações e modelo do Comitê Gestor de Proteção de Dados, adequando-o às necessidades e peculiaridades da Epagri.

5.6.2 Departamento Estadual de Marketing e Comunicação (DEMC)

● Apoiar, coordenar e executar atividades de editoração técnica com fins institucionais, informativos ou educativos, relacionadas ao respectivo Plano;

● Produzir e editar conteúdo jornalístico relacionado à divulgação do respectivo Plano.

5.6.3 Encarregado de Dados

● Garantir que as cláusulas contratuais estejam em conformidade com a LGPD e as orientações da Agência Nacional de Proteção de Dados (ANPD);

● Monitorar o cumprimento das normas previstas nos contratos no que diz respeito à proteção de dados pessoais;

● Fornecer orientação e capacitação aos gestores e demais envolvidos sobre o cumprimento das cláusulas de proteção de dados.

5.6.4 Gestores das Unidades/Gestores dos Contratos

● Garantir que os contratos sob sua responsabilidade incluam as cláusulas de proteção de dados e estejam alinhados com as diretrizes deste Plano;

● Promover a revisão de contratos vigentes para adequação à LGPD, quando necessário;

● Comunicar imediatamente ao DJUR e ao DPO quaisquer situações de não conformidade identificadas.

5.6.5 Usuários e Fiscais dos Contratos

● Manter o compromisso com o cumprimento das diretrizes deste Plano em suas atividades diárias;

● Reportar quaisquer incidentes de segurança envolvendo dados pessoais ao superior hierárquico e ao Encarregado de Dados (DPO);

● Participar de treinamentos e atualizações relacionados à LGPD e à segurança da informação promovidos pela Epagri.

ANEXO IV.1 - CLÁUSULA DE PROTEÇÃO DE DADOS PESSOAIS E LGPD

O presente documento versa sobre orientações de cunho **recomendatório** visando à conformidade de cláusulas contratuais no tocante à proteção de dados pessoais.

Ressalta-se que devem ser respeitadas a **essência** e a **finalidade** da Epagri e observadas as **características e peculiaridades existentes em cada contrato**.

CLÁUSULA #NÚMERO# – PROTEÇÃO DE DADOS PESSOAIS E LGPD

#NÚMERO#. – A CONTRATADA declara que tem ciência da existência da Lei federal nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais) e se compromete a adequar todos os procedimentos internos ao disposto na legislação, com o intuito de proteger os dados pessoais que lhe forem repassados, cumprindo, a todo momento, as normas de proteção de dados pessoais, jamais colocando, por seus atos ou por sua omissão, a EPAGRI em situação de violação de tais regras.

#NÚMERO#. – A CONTRATADA declara que designou encarregado(a) de tratamento de dados pessoais, nos termos do § 1º do art. 41 da Lei federal nº 13.709, de 2018, conforme indicado na sua página eletrônica e se compromete a manter a Epagri informada sobre os dados atualizados do contato de seu encarregado de tratamento de dados pessoais, sempre que for substituído, independentemente das alterações em sua página eletrônica. Caso a CONTRATADA seja uma microempresa ou empresa de pequeno porte, dispensada de indicar encarregado(a), na forma do § 3º do art. 41 da LGPD e resolução da Agência Nacional de Proteção de Dados (ANPD), os seus agentes de tratamento não ficarão isentos do cumprimento de outras disposições legais e regulamentares relativas à proteção de dados pessoais.

#NÚMERO#. – A CONTRATADA somente poderá tratar dados pessoais dos usuários dos serviços contratados nos limites e finalidades exclusivas do cumprimento de suas obrigações, com base no presente contrato e jamais para qualquer outra finalidade.

#NÚMERO#. – A CONTRATADA se certificará de que seus empregados, representantes e prepostos agirão de acordo com o contrato, com as leis de proteção de dados e eventuais instruções transmitidas pela Epagri, comprometendo-se a manter o

sigilo e a confidencialidade dos dados pessoais e dos dados pessoais sensíveis repassados em decorrência da execução do objeto contratual, em consonância com a Lei federal nº 13.709, de 2018, certificando-se a CONTRATADA de que seus empregados, representantes e prepostos assumam compromisso de confidencialidade ou estejam sujeitos a obrigações legais de confidencialidade.

#NÚMERO#. – Se o titular dos dados ou terceiros solicitarem informações à CONTRATADA relativas ao tratamento de dados pessoais que detiver em decorrência do presente contrato, a CONTRATADA submeterá esse pedido à apreciação da Epagri, não podendo, sem instruções prévias da **Epagri**, transferir, compartilhar e/ou garantir acesso aos dados pessoais que detenha por força deste contrato; sendo, em regra, vedada a transferência das informações a outras pessoas físicas ou jurídicas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do próprio contrato. Se a solicitação for realizada por autoridade de proteção de dados, a CONTRATADA informará imediatamente à **Epagri** sobre tal pedido e suas decorrências.

#NÚMERO#. – A CONTRATADA prestará assistência à Epagri no cumprimento das obrigações previstas nas leis de proteção de dados, quando relacionadas ao objeto contratual, especialmente nos casos em que for necessária a assistência da CONTRATADA para que a Epagri cumpra suas obrigações, incluindo aquelas relativas à segurança do tratamento, violações de dados pessoais, avaliação de impacto de proteção de dados e consulta prévia a autoridades de proteção de dados, abrangendo pedidos de acesso, retificação, bloqueio, restrição, apagamento, portabilidade de dados ou o exercício de quaisquer outros direitos dos titulares de dados com base nas leis aplicáveis à proteção de dados.

#NÚMERO#. – Quando solicitada, a CONTRATADA fornecerá à Epagri, no prazo de **2 (dois) dias úteis**, todas as informações necessárias para comprovar a conformidade das obrigações da CONTRATADA previstas neste contrato com as leis de proteção de dados, inclusive para fins de elaboração de relatórios de impacto de proteção e riscos de uso de dados pessoais.

#NÚMERO#. – A CONTRATADA prestará assistência à Epagri no cumprimento de suas outras obrigações de acordo com as leis de proteção de dados nos casos em que estiver implícita a assistência da CONTRATADA e/ou nos casos em que for necessária a assistência da CONTRATADA para que a Epagri cumpra suas obrigações, incluindo aquelas

relativas à segurança do tratamento, violações de dados pessoais, avaliação de impacto de proteção de dados e consulta prévia a autoridades de proteção de dados.

#NÚMERO#. – A CONTRATADA fica obrigada a comunicar à Epagri, por escrito, em até **2 (dois) dias úteis**, a contar do momento em que tomou ciência da violação, ou em menor prazo, se assim vier a recomendar ou determinar a **ANPD**, qualquer incidente de acesso não autorizado aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da LGPD.

#NÚMERO#. – A CONTRATADA indenizará a Epagri em virtude do não cumprimento das obrigações previstas nas leis, normas, regulamentos e recomendações das autoridades de proteção de dados com relação ao presente contrato, de quaisquer danos, prejuízos, custos e despesas, incluindo-se honorários advocatícios, multas, penalidades e eventuais dispêndios investigativos relativos a demandas administrativas ou judiciais propostas em face da Epagri a esse título.

#NÚMERO#. – A CONTRATADA declara estar ciente da Política de Privacidade e Proteção de Dados Pessoais da Epagri, disponível no *link*: https://epagri.sc.gov.br/index.php/politica-de-privacidade/

ANEXO IV.2 - MINUTA DE TERMO ADITIVO DE CLÁUSULA DE PROTEÇÃO DE DADOS PESSOAIS E LGPD

I - DA ALTERAÇÃO

Considerando o advento da Lei federal nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais) e a necessidade de que os contratos estejam em conformidade com essa legislação, devem ser incluídas as seguintes cláusulas no contrato original:

Cláusula 15ª (se serviço) e Cláusula 16ª (se fornecimento de produtos) – Proteção de Dados Pessoais e LGPD

A CONTRATADA declara que tem ciência da existência da **Lei federal nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais)** e se compromete a adequar todos os procedimentos internos ao disposto na legislação, com o intuito de proteger os dados pessoais que lhe forem repassados, cumprindo, a todo momento, as normas de proteção de dados pessoais, jamais colocando, por seus atos ou por sua omissão, a Epagri em situação de violação de tais regras.

§ 1º. A CONTRATADA declara que designou **encarregado(a)** de tratamento de dados pessoais, nos termos do § 1º do art. 41 da Lei federal nº 13.709, de 2018, conforme indicado na sua página eletrônica e se compromete a manter a **Epagri** informada sobre os dados atualizados do contato de seu encarregado de tratamento de dados pessoais, sempre que for substituído, independentemente das alterações em sua página eletrônica. **Caso a CONTRATADA seja uma microempresa ou empresa de pequeno porte, dispensada de indicar encarregado(a), na forma do § 3º do art. 41 da LGPD e resolução da Autoridade Nacional de Proteção de Dados (ANPD), os seus agentes de tratamento não ficarão isentos do cumprimento de outras disposições legais e regulamentares relativas à proteção de dados pessoais.**

§ 2º. A CONTRATADA somente poderá tratar dados pessoais dos usuários dos serviços contratados nos limites e finalidades exclusivas do cumprimento de suas obrigações, com base no presente contrato e jamais para qualquer outra finalidade.

§ 3º. A CONTRATADA se certificará de que seus empregados, representantes e prepostos agirão de acordo com o contrato, com as leis de proteção de dados e eventuais instruções transmitidas pela Epagri, comprometendo-se a manter o sigilo e a confidencialidade dos dados pessoais e dos **dados pessoais sensíveis** repassados em decorrência da execução do objeto contratual, em consonância com a Lei federal nº 13.709, de 2018, certificando-se a CONTRATADA de que seus empregados, representantes

e prepostos assumam compromisso de confidencialidade ou estejam sujeitos a obrigações legais de confidencialidade.

§ 4º. Se o titular dos dados ou terceiros solicitarem informações à CONTRATADA relativas ao tratamento de dados pessoais que detiver em decorrência do presente contrato, a CONTRATADA submeterá esse pedido à apreciação da Epagri, não podendo, sem instruções prévias da Epagri, transferir, compartilhar e/ou garantir acesso aos dados pessoais que detenha por força deste contrato; sendo, em regra, vedada a transferência das informações a outras pessoas físicas ou jurídicas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do próprio contrato. Se a solicitação for realizada por autoridade de proteção de dados, a CONTRATADA informará imediatamente à Epagri sobre tal pedido e suas decorrências.

§ 5º. A CONTRATADA prestará assistência à Epagri no cumprimento das obrigações previstas nas leis de proteção de dados, quando relacionadas ao objeto contratual, especialmente nos casos em que for necessária a assistência da CONTRATADA para que a Epagri cumpra suas obrigações, incluindo aquelas relativas à segurança do tratamento, violações de dados pessoais, avaliação de impacto de proteção de dados e consulta prévia a autoridades de proteção de dados, abrangendo pedidos de acesso, retificação, bloqueio, restrição, apagamento, portabilidade de dados ou o exercício de quaisquer outros direitos dos titulares de dados com base nas leis aplicáveis à proteção de dados.

§ 6º. Quando solicitada, a CONTRATADA fornecerá à Epagri, no prazo de **2 (dois) dias úteis**, todas as informações necessárias para comprovar a conformidade das obrigações da CONTRATADA previstas neste contrato com as leis de proteção de dados, inclusive para fins de elaboração de relatórios de impacto de proteção e riscos de uso de dados pessoais.

§ 7º. A CONTRATADA prestará assistência à Epagri no cumprimento de suas outras obrigações de acordo com as leis de proteção de dados nos casos em que estiver implícita a assistência da CONTRATADA e/ou nos casos em que for necessária a assistência da CONTRATADA para que a Epagri cumpra suas obrigações, incluindo aquelas relativas à segurança do tratamento, violações de dados pessoais, avaliação de impacto de proteção de dados e consulta prévia a autoridades de proteção de dados.

§ 8º. A CONTRATADA fica obrigada a comunicar à Epagri, por escrito, em até **2 (dois) dias úteis**, a contar do momento em que tomou ciência da violação, ou em menor prazo, se assim vier a recomendar ou determinar a **ANPD**, qualquer incidente de acesso não autorizado aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da LGPD.

§ 9º. A CONTRATADA indenizará a Epagri em virtude do não cumprimento das

obrigações previstas nas leis, normas, regulamentos e recomendações das autoridades de proteção de dados com relação ao presente contrato, de quaisquer danos, prejuízos, custos e despesas, incluindo-se honorários advocatícios, multas, penalidades e eventuais dispêndios investigativos relativos a demandas administrativas ou judiciais propostas em face da Epagri a esse título.

§ 10. A CONTRATADA declara estar ciente da Política de Privacidade e Proteção de Dados Pessoais da Epagri, disponível no *link*: https://epagri.sc.gov.br/index.php/politica-de-privacidade/

6 ANEXO V - PLANO DE CONTROLE DE ACESSO À INFORMAÇÃO

6.1 Apresentação

A Epagri lida com informações confidenciais e públicas compartilhadas com outras entidades, como governos e o setor privado, conforme a legislação. A proteção e o controle de acesso a essas informações são fundamentais para garantir a segurança, confidencialidade, disponibilidade, autenticidade e integridade dos dados pessoais, em cumprimento à Lei Geral de Proteção de Dados Pessoais (LGPD).

Este Plano estabelece os processos e responsabilidades para o controle de acesso às informações da Epagri.

6.2 Objetivo

O Plano de Controle de Acesso à Informação visa estabelecer controles de identificação, autenticação e autorização de acesso às informações custodiadas pela Epagri, prevenindo acessos não autorizados que possam resultar em destruição, perda, alteração, comunicação ou outra forma de tratamento inadequado ou ilícito.

O Plano abrange tanto o acesso lógico (sistemas e redes) quanto o acesso físico (ambientes e equipamentos).

6.3 Campo de Aplicação

Este Plano aplica-se:

- Todas as informações tratadas pela Epagri, independentemente do meio (digital ou físico).
- Todos os usuários e unidades da Epagri.
- Sistemas de informação e ambientes físicos da Epagri.

6.4 Legislação

- Lei federal nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- Resolução CD/ANPD nº 15, de 2024 (regulamento de comunicação de incidente de segurança);
- Resolução CD/ANPD nº 18, de 2024 (regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais);

- Decreto estadual nº 1.892, de 2022 (atribuições e requisitos da função de encarregado pelo tratamento de dados pessoais);
- Instrução Normativa SEA nº 20, de 2021 (Política de Segurança da Informação – POSIN).

6.5 Atribuições e Responsabilidades

6.5.1 Departamento Estadual de Gestão da Tecnologia da Informação (DEGTI)

- Estabelecer e manter inventários das contas de acesso e dos sistemas de autenticação e autorização;
- Gerir e centralizar os processos de criação, manutenção, bloqueio e revogação de contas de acesso;
- Implementar e monitorar o uso de autenticação de multifatores (MFA) para acesso remoto e para contas administrativas;
- Controlar e revisar o acesso a sistemas e dados confidenciais, garantindo que os usuários tenham apenas os privilégios necessários, conforme solicitações das demais unidades;
- Manter registro de todos os acessos a sistemas críticos e analisar *logs* periodicamente para detectar acessos irregulares;
- Configurar bloqueio automático de sessões após períodos de inatividade nos dispositivos.

6.5.2 Departamento Estadual de Gestão de Pessoas (DEGP)

- Cadastrar os novos usuários no Sistema de Colaboradores, ou outro que vier substituí-lo;
- Comunicar ao DEGTI sobre transferência de usuários para outra unidade da Empresa, alteração de cargo ou função, de desligamento e afastamentos, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos;
- Comunicar ao DEGTI a movimentação (transferência, alteração de cargo ou função, desligamento e afastamentos) de usuários não concursados (como bolsistas, aprendizes e terceirizados). A comunicação deve ser feita após o recebimento da informação prévia do Gestor responsável pela Unidade ou Departamento de lotação.

6.5.3 Departamento Estadual de Gestão Operacional (DEGOP)

● Comunicar ao DEGTI eventuais desligamentos, férias, licenças e demais afastamentos de funcionários terceirizados para bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos;

● Auxiliar a implementação e o monitoramento dos controles de acesso físico aos ambientes da Epagri.

6.5.4 Departamento Estadual de Marketing e Comunicação (DEMC)

● Apoiar, coordenar e executar atividades de editoração técnica com fins institucionais, informativos ou educativos, relacionadas ao respectivo Plano;

● Produzir e editar conteúdo jornalístico relacionado à divulgação do respectivo Plano.

6.5.5 Encarregado de Dados

● Exercer as atribuições previstas no Regimento Interno da Epagri, Decreto estadual nº 1.892, de 2022 e Resolução CD/ANPD nº 18/2024 ou normas supervenientes;

● Orientar e garantir que o tratamento de dados pessoais siga as diretrizes da LGPD;

● Monitorar e comunicar incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais à Agência Nacional de Proteção de Dados (ANPD), na forma da Resolução CD/ANPD nº 15/2024 e Plano de Resposta a Incidentes de Segurança da Epagri.

6.5.6 Usuários

● Utilizar os sistemas e ambientes da Epagri em conformidade com as normas de segurança da informação estabelecidas;

● Manter a confidencialidade de suas credenciais de acesso (*login* e senha).

● Reportar ao DEGTI qualquer incidente de segurança ou suspeita de uso indevido de sua conta;

Reportar **imediatamente** incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais ao superior hierárquico e Encarregado de Dados, conforme o **Plano de Resposta a Incidentes de Segurança**;

● Bloquear sua estação de trabalho quando ausentes, para prevenir acessos indevidos;

● Não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

● Utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

● Assinar o Termo de Responsabilidade da Política de Tecnologia de Informação e Comunicação da Epagri quanto à utilização da respectiva conta de acesso.

6.5.7 Gestores das Unidades da Epagri

● Solicitar ao DEGTI a alteração ou revogação de acessos indevidos dos usuários das unidades;

● Solicitar ao DEGTI os acessos e privilégios necessários aos sistemas para os usuários de sua responsabilidade;

● Reportar ao DEGTI qualquer incidente de segurança ou suspeita de uso indevido de sua conta;

● Reportar **imediatamente** incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais ao Encarregado de Dados, conforme o Plano de Resposta a Incidentes de Segurança;

● Comunicar ao DEGP a transferência, alteração de cargo ou função, desligamento e afastamentos de usuários bolsistas, aprendizes ou terceirizados das unidades de lotação.

6.5.8 Diretoria Executiva

● Aprovar as atualizações e alterações deste Plano;

● Assegurar a alocação de recursos necessários para a execução deste Plano.

6.6 Acesso Lógico

6.6.1 Controles de Acesso Lógico

● O acesso aos recursos da rede e aos sistemas corporativos será controlado por um sistema de controle de acesso baseado em perfis, centralizado pelo DEGTI, por meio de um serviço de diretório ou provedor de *Single Sign On (SSO) – login* único.

● O MFA será utilizado nas seguintes hipóteses:

- para acessos remotos;
- para acesso às aplicações corporativas ou de terceiros que estejam hospedados em fornecedores.

● Os privilégios de acesso dos usuários à Rede e sistemas devem ser definidos pela unidade requisitante à qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas;

● Qualquer alteração nos privilégios de acesso deve ser documentada e justificada pela unidade requisitante;

● O acesso a sistemas que tratam dados pessoais deve ser restrito ao mínimo necessário, em conformidade com os princípios da **necessidade, finalidade e adequação** da LGPD;

● O acesso remoto deve ser realizado por meio de **VPN** – **Rede Virtual Privada**, ou por sistema que venha a substituir este meio após as devidas autorizações;

● A criação de novas contas deve seguir o padrão de nomeação: primeiro nome + último sobrenome, sendo excepcionalmente alterada em caso de duplicidade;

● **A falta de solicitação de transferência de usuários para outra unidade e/ou setor da Empresa, alteração de cargo ou função, ou comunicação de desligamento e afastamentos sujeita o dirigente à responsabilização por eventuais ações realizadas pelo usuário que deveria ter seu perfil de acesso revogado ou bloqueado, sem prejuízo da responsabilização do usuário.**

6.6.2 Gestão de Contas de Acesso

● O DEGTI deve manter um inventário atualizado das contas de acesso de usuário, corporativas e de serviço, contendo informações sobre a unidade proprietária, data de criação, de renovação e últimas alterações;

● As contas de acesso lógico devem ser **bloqueadas** nas seguintes situações:

- após **5 (cinco)** tentativas de *login* incorreto;
- caso não efetue a troca da senha no prazo estabelecido;
- solicitação do superior imediato do usuário com a devida justificativa;
- quando da suspeita de mau uso dos serviços disponibilizados pela Epagri ou descumprimento da Política de Segurança da Informação (POSIN) e normas correlatas em vigência.

● O uso compartilhado de identificador de usuário somente será permitido por razões operacionais ou de negócios e deverá ser aprovado e documentado;

● O DEGTI deve, sempre que possível, priorizar a revogação/desativação de contas ao invés de exclusão, com o objetivo de manter dados e *logs* para possíveis auditorias;

● O uso de identificação (*login*) com acesso no perfil de administrador é permitido somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação, observado o seguinte:

○ Somente os técnicos do DEGTI ou colaboradores de outras unidades que estejam enquadrados nos cargos de Agente de Tecnologia da Informação e Comunicação e ou Suporte Técnico em Informática, devidamente identificados e habilitados, terão senha com privilégio de **administrador** nos equipamentos locais, equipamentos de rede e sistemas. Exceções a esta regra somente serão permitidas com expressa autorização do responsável pela unidade do usuário, com anuência do DEGTI, através de termo de responsabilidade;

○ Na necessidade de utilização de *login* com privilégio de administrador do equipamento, o usuário deverá encaminhar solicitação para o DEGTI, que poderá negar os casos em que entender desnecessária a utilização;

○ Se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar, desenvolver, modificar ou remover qualquer programa sem autorização formal do DEGTI;

○ Salvo para atividades específicas do DEGTI, não será concedida, para um mesmo usuário, identificação (*login*) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede;

○ O DEGTI deve implementar o MFA para todas as contas de administrador;

○ O DEGTI deve restringir os privilégios de administrador a contas de administradores dedicados aos ativos de informação, para que o usuário com privilégio de administrador não consiga realizar atividades gerais de computação, como navegação na internet, e-mail e uso do pacote de produtividade. Essas atividades deverão ser realizadas preferencialmente a partir da conta primária não privilegiada do usuário.

6.6.3 Política de Senhas

● Senhas de acesso devem ser complexas, e o padrão de tamanho e composição, bem como a periodicidade de troca devem seguir a determinação do DEGTI;

● As senhas de acesso serão renovadas periodicamente de acordo com definição do DEGTI, devendo o usuário ser informado antecipadamente a fim de que ele próprio possa efetuar a mudança;

● O DEGTI fornecerá senhas temporárias para novos usuários ou em caso de esquecimento, as quais deverão ser alteradas no primeiro ou no próximo acesso.

6.7 Acesso Físico

6.7.1 Controle de Acesso a Ambientes Seguros

● O acesso a áreas que armazenam dados confidenciais será restrito a pessoal autorizado e monitorado por mecanismos de controle, como câmeras, fechaduras digitais e biometria;

● O DEGTI, em conjunto com o DEGOP, deve realizar testes periódicos nos sistemas de controle de acesso físico para garantir sua eficácia;

● Os ativos de armazenamento e tratamento de dados que se encontrem fora da Epagri devem ser protegidos contra perda, roubos, danos e acesso físico não autorizados, conforme as seguintes diretrizes:

- não deixar o ativo sem vigilância em locais públicos e inseguros;
- proteger o ativo contra riscos associados à visualização de informações por outra pessoa;
- implementar as funcionalidades de rastreamento e limpeza remota.

6.7.2 Processo de Autorização de Acesso Físico

● O acesso de visitantes, fornecedores e prestadores de serviço a áreas restritas deve ser autorizado previamente pelo DEGTI e ser supervisionado durante toda a sua permanência;

● O departamento/gerência na qual os servidores e centros de dados estão alocados deve manter registros físicos ou eletrônicos de todos os acessos a essas áreas. Caso não haja um responsável pelo local, o controle desse acesso será de responsabilidade do DEGTI.

6.8 Acesso Biométrico

● A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico;

● A Epagri deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente;

● A Epagri somente poderá compartilhar banco de dados biométricos com terceiros se forem atendidas as bases legais da LGPD e com prévio parecer do Encarregado de Dados emitido no SGP-e.

6.9 Monitoramento e Revisão

6.9.1 Auditorias de Acesso

● O DEGTI deve realizar auditorias periódicas para verificar a conformidade dos acessos aos sistemas e ambientes;

Incidentes de segurança e acessos indevidos devem ser imediatamente comunicados ao Encarregado de Dados. O Encarregado de Dados deve comunicar incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais à ANPD, na forma da Resolução CD/ANPD nº 15/2024 e Plano de Resposta a Incidentes de Segurança da Epagri.

6.9.2 Revisão de Acessos

● O DEGTI deve revisar o inventário de contas de terceiros, corporativas e de sistemas a cada **180 (cento e oitenta) dias**;

● A revisão também se aplica a contas de administradores, que devem ser mantidas apenas enquanto necessárias.

6.10 Disposições finais

Este Plano entra em vigor na data de sua aprovação pela Diretoria Executiva da Epagri e deve ser revisado sempre que houver necessidade para adequação às necessidades da Empresa, adaptação a novas tecnologias, atendimento a requisitos legais e mudanças nos processos internos.

7 ANEXO VI - PLANO DE CONSENTIMENTO DE DADOS

7.1 Apresentação

O Plano de Consentimento de Dados estabelece diretrizes, responsabilidades e procedimentos para a obtenção, registro e gestão do consentimento dos titulares de dados pessoais, assegurando a transparência e a proteção de seus direitos.

Nas atividades da Epagri, o tratamento de dados pessoais é geralmente realizado com fundamento em outras bases legais da Lei Geral de Proteção de Dados Pessoais (LGPD), como cumprimento de obrigações legais ou regulatórias; execução de políticas públicas; execução de contratos; e exercício regular de direitos em processos judiciais ou administrativos, **as quais independem de consentimento do titular de dados.**

O consentimento, embora relevante, é menos frequente na Epagri, empresa pública que presta serviços públicos. No entanto, quando o tratamento de dados for realizado com base no consentimento (conforme art. 7º, I e art. 11, I, ambos da LGPD), este Plano deve ser integralmente observado.

7.2 Objetivos

● Assegurar que o uso do consentimento como base legal para o tratamento de dados pessoais pela Epagri seja realizado de form**a clara, livre, informada** e em conformidade com a LGPD;

● Garantir a transparência no uso dos dados pessoais coletados;

● Assegurar que os titulares estejam cientes das **finalidades** e formas de tratamento de seus dados;

● Prover diretrizes para a utilização adequada da base legal de consentimento no âmbito da Epagri.

7.3 Campo de Aplicação

Este Plano se aplica a todas as unidades, usuários e atividades da Epagri que envolvam a coleta, o armazenamento e o tratamento de dados pessoais com base no consentimento dos titulares de dados.

7.4 Legislação e Boas Práticas

• Lei federal nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

• Resolução CD/ANPD nº 18, de 2024 (Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais);

• Decreto estadual nº 1.892, de 2022 (atribuições e requisitos da função de encarregado pelo tratamento de dados pessoais);

• Instrução Normativa SEA nº 20, de 2021 (Política de Segurança da Informação – POSIN).

7.5 Diretrizes

7.5.1 Quando Utilizar a Hipótese de Consentimento:

- **Eventos e Programas de Capacitação**
  - **Situação:** em eventos, *workshops* e programas de capacitação em que são coletados dados pessoais dos participantes para fins de registro, avaliação e certificação;
  - **Exemplo:** registro de participantes em um *workshop* sobre técnicas de cultivo sustentável, em que são coletadas informações pessoais como nome, contato e perfil profissional;
  - **Justificativa:** o consentimento é necessário para assegurar que os dados dos participantes sejam utilizados apenas para os fins especificados e que eles estejam cientes de como suas informações serão tratadas;
  - **Observação:** o consentimento não será necessário se o evento ou programa de capacitação estiver atrelado à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, pois o tratamento se enquadrará em outra base legal da LGPD.

- ***Publicações e Divulgação de Resultados***
  - **Situação:** quando a Epagri deseja utilizar dados pessoais em publicações ou relatórios públicos;
  - **Exemplo:** divulgação de estudos de caso que incluem dados pessoais dos agricultores participantes;
  - **Justificativa:** o consentimento garante que os titulares dos dados estejam cientes de que suas informações serão divulgadas publicamente e para quais finalidades, protegendo sua privacidade e direitos;

○ **Observação:** o consentimento não será necessário se a pesquisa for realizada com anonimização de dados, pois o tratamento se enquadrará em outra base legal da LGPD.

● ***Outras hipóteses de tratamento que não se enquadrem nas bases legais dos arts. 7º e 11 da LGPD que independem de consentimento***

Observação: sempre que o tratamento dos dados pessoais não puder ser enquadrado nas bases legais do art. 7º, incisos II a X, e 11, II, da LGPD, que **independem de consentimento**, o titular de dados deve autorizar o tratamento de seus dados pessoais por meio do Termo de consentimento – modelo padrão. Em caso de dúvidas, a unidade deve consultar o Encarregado de Dados (dpo@epagri.sc.gov.br)

7.5.2 Princípios do Consentimento

● **Transparência:** informar claramente as finalidades e os meios de tratamento;

● **Livre Escolha:** consentimento dado sem pressões ou quaisquer outros vícios de consentimento (erro, dolo, coação, lesão ou estado de perigo);

● **Especificidade:** válido apenas para as finalidades especificadas. Autorizações genéricas para o tratamento de dados pessoais são nulas;

● **Informação:** detalhes suficientes para decisão informada;

● **Revogabilidade:** possibilidade de revogação a qualquer momento.

7.5.3 Registro e Gestão do Consentimento

7.5.3.1 Termo de consentimento

O consentimento do titular deve ser prestado por escrito ou por outro meio que demonstre de forma inequívoca a manifestação de sua vontade. O consentimento pode se dar das seguintes formas:

Modelo padrão de termo de consentimento: o consentimento pode ser fornecido por meio do modelo constante na Cadeia de Valor (Termo de Consentimento) devendo uma cópia assinada ser encaminhada ao Encarregado de Dados no endereço eletrônico dpo@epagri.sc.gov.br;

● Os termos de consentimento encaminhados serão anexados em SGP-e específico para tal ato;

● **Outros modelos de consentimento**: também é possível utilizar outros documentos para o consentimento, desde que previamente analisados e aprovados pelo

Encarregado de Dados;

● **Consentimento em contrato**: quando o consentimento for incluído em contrato, este deverá constar em uma cláusula destacada das demais, em conformidade com o art. 8º, § 1º, da LGPD.

Além disso, o termo de consentimento deve atender aos seguintes requisitos:

● Ser claro, compreensível e acessível;

● Ser escrito em linguagem simples, garantindo a plena compreensão do titular;

● Se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, a Epagri deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações;

● O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

O gerenciamento dos termos de consentimento e os procedimentos de controle podem ser revisados ou atualizados a qualquer momento, visando à melhoria contínua dos processos.

7.5.3.2 Sistemas Digitais

A Epagri poderá implementar mecanismos de consentimento em plataformas digitais, como *websites* e aplicativos, assegurando a clareza das informações e a facilidade de uso.

7.5.4 Informações a Serem Fornecidas ao Titular

● **Finalidade do Tratamento:** explicar claramente por que os dados estão sendo coletados e como serão utilizados;

● **Período de Retenção:** informar por quanto tempo os dados serão mantidos;

Direitos dos Titulares e contato para dúvidas: explicar os direitos dos titulares previstos na LGPD, incluindo acesso, correção, portabilidade e eliminação dos dados, bem como fornecer informações de contato para que os titulares possam esclarecer dúvidas ou exercer seus direitos. Essas informações podem consistir em *link* direcionado à Política de Privacidade e Proteção de Dados Pessoais da Epagri.

7.5.5 Revogação do Consentimento

Processo de Revogação: o titular pode revogar seu consentimento a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado. Para tanto, basta que o titular encaminhe a solicitação de revogação por meio do serviço "Solicitar Atendimento dos Direitos do Titular dos Dados Pessoais no âmbito do Poder Executivo Estadual (LGPD)", disponível em: https://www.sc.gov.br/servicos/solicitar-atendimento-lgpd

● **Consequências da Revogação:** informar aos titulares as possíveis consequências da revogação do consentimento, como a interrupção de determinados serviços;

O titular de dados também pode se opor ao tratamento realizado pela Epagri com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento da LGPD. A oposição ao tratamento também pode ser encaminhada por meio do serviço "Solicitar Atendimento dos Direitos do Titular dos Dados Pessoais no âmbito do Poder Executivo Estadual (LGPD)", disponível em: https://www.sc.gov.br/servicos/solicitar-atendimento-lgpd

7.6 Atribuições e Responsabilidades

7.6.1 Diretoria Executiva

● Demonstrar o comprometimento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais, conforme o art. 50, § 2º, inciso I, da LGPD;

● Apoiar e promover a cultura de proteção de dados na Epagri;

● Assegurar a alocação de recursos necessários para a execução deste Plano.

7.6.2 Encarregado de Proteção de Dados (DPO)

● Coordenar o desenvolvimento e a execução deste Plano e revisar os materiais periodicamente;

● Conduzir treinamentos e orientar os usuários a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

● Propor à Diretoria Executiva a revisão deste Plano, quando necessário.

7.6.3 Departamento Estadual de Gestão da Tecnologia da Informação (DEGTI)

● Prover ferramentas tecnológicas para otimizar a obtenção e a gestão do consentimento dos titulares de dados.

7.6.4 Departamento Jurídico (DJUR)

● Apoiar na revisão jurídica do modelo Termo de Consentimento;

● Orientar o Encarregado de Dados e os dirigentes responsáveis pelas Unidades de gestão sobre matéria jurídica envolvendo proteção de dados pessoais;

● Emitir informações e pareceres sobre questões de natureza jurídica envolvendo dados pessoais.

7.6.5. Departamento Estadual de Marketing e Comunicação (DEMC)

● Apoiar, coordenar e executar atividades de editoração técnica com fins institucionais, informativos ou educativos, relacionadas ao respectivo Plano.

● Produzir e editar conteúdo jornalístico relacionado à divulgação do respectivo Plano.

7.6.6 Gestores de Unidades da Epagri

● Promover e fomentar a participação das suas equipes nos treinamentos sobre proteção de dados pessoais;

● Reforçar o cumprimento das diretrizes sobre proteção de dados pessoais nas unidades sob sua gestão.

7.6.7 Usuários

● Participar dos treinamentos e programas de conscientização, aplicando as regras deste Plano nas suas atividades laborais;

● Reportar inconsistências ou falhas nos processos de consentimento ao Encarregado de Dados;

● Reportar incidentes de segurança imediatamente ao superior hierárquico e

Encarregado de Dados, conforme o Plano de Resposta a Incidentes de Segurança.

7.7 Disposições finais

- Este Plano deve ser revisado periodicamente, considerando atualizações legislativas e avanços nas melhores práticas;
- Qualquer alteração nas finalidades de tratamento requer nova coleta de consentimento.

8 ANEXO VII - PLANO DE PROTEÇÃO DE DADOS PESSOAIS DA EPAGRI

8.1 Apresentação

O Plano de Proteção de Dados Pessoais da Empresa de Pesquisa Agropecuária e Extensão Rural de Santa Catarina (Epagri) integra a Política de Segurança da Informação (POSIN) e tem como finalidade estabelecer diretrizes, normas e procedimentos para o tratamento seguro e adequado de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei Federal nº 13.709/2018).

8.2 Objetivos

O Plano tem por objetivos:

- Salvaguardar dados pessoais e dados pessoais sensíveis tratados pela Epagri;
- Preservar a integridade, confidencialidade e disponibilidade dessas informações;
- Prevenir o uso indevido, vazamentos ou acessos não autorizados;
- Assegurar o tratamento de dados com base legal adequada, finalidade legítima e transparência;
- Promover o cumprimento das obrigações previstas na LGPD;
- Estimular a conscientização de todos os usuários da Epagri sobre a importância da proteção de dados.

8.3 Campo de Aplicação

Aplica-se a todas as áreas, departamentos e usuários da Epagri e ao tratamento de dados pessoais em qualquer formato (físico ou digital), em todas as etapas: coleta, uso, armazenamento, compartilhamento, descarte, etc.

Este Plano também se aplica a operadores e a eventuais terceiros com acesso ou envolvimento em operações com dados pessoais em nome da Epagri.

8.4 Legislação e Boas Práticas

- Este Plano está fundamentado na seguinte legislação e em normas reconhecidas Constituição Federal de 1988 (especialmente o art. 5º, incisos X e XII);

- Lei federal nº 12.527, de 2011 (Lei de Acesso à Informação – LAI);
- Lei federal n º 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- Lei estadual nº 19.450, de 2025 (princípios e diretrizes para o uso da inteligência artificial no âmbito da Administração Pública);
- Resolução CD/ANPD nº 18, de 2024 (Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais);
- Decreto estadual nº 1.892, de 2022 (atribuições e requisitos da função de encarregado pelo tratamento de dados pessoais);
- Instrução Normativa SEA nº 20, de 2021 (Política de Segurança da Informação – POSIN);
- ABNT NBR ISO/IEC 27001 (Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação);
- Normas da Agência Nacional de Proteção de Dados (ANPD).

8.5 Diretrizes

8.5.1 Compartilhamento com Terceiros

- Terceiros só podem acessar um banco de dados pessoais específico da Epagri se houver base legal, necessidade, finalidade legítima e parecer favorável do Encarregado de Dados Pessoais (via SGP-e), conforme o Plano de Acesso à Informação da POSIN;
- Os contratos devem prever cláusulas específicas sobre proteção de dados e responsabilidade por incidentes, conforme o Plano de Gestão de Contratos da POSIN.

8.5.2 Inventário de Dados

- A Epagri manterá inventário atualizado dos dados pessoais tratados, incluindo: processos vinculados, finalidade, base legal, titulares, dados pessoais sensíveis, tempo de retenção, medidas de segurança e compartilhamentos.

8.5.3 Registro de Atividades

Todos os tratamentos de dados, consentimentos, treinamentos, auditorias e incidentes devem ser devidamente registrados no SGP-e, garantindo rastreabilidade e transparência em eventuais auditorias ou demandas da ANPD.

8.5.4 Comunicação Interna

● Toda alteração na POSIN ou neste Plano deve ser comunicada de forma clara e acessível, por e-mail, boletim eletrônico interno, *intranet* ou meios físicos, conforme o perfil do público, em linguagem simples.

8.5.5 Avaliação de Maturidade

● A Epagri poderá aplicar questionários e diagnósticos para avaliar a maturidade em segurança da informação e proteção de dados, com base em padrões internacionais de segurança da informação, como a ABNT NBR ISO/IEC 27001.

8.6 Atribuições e Responsabilidades

8.6.1 Diretoria Executiva

● Garantir os recursos necessários à implementação da LGPD e execução deste Plano.

8.6.2 Encarregado de Dados Pessoais (DPO)

● Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

● Receber comunicações da ANPD e adotar providências;

● Orientar os usuários e os terceiros que se relacionam com a Epagri a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

● Emitir pareceres sobre qualquer demanda interna relacionada ao tratamento de dados pessoais, como uso, compartilhamento, descarte, base legal, atendimento a titulares, entre outros;

● Monitorar o cumprimento da LGPD na Epagri;

● Promover ações de sensibilização, treinamento e comunicação interna para conscientizar os colaboradores sobre a proteção de dados pessoais;

● Atualizar o inventário de dados pessoais periodicamente ou sempre que houver mudanças significativas nos processos de tratamento de dados;

● Manter o controle de indicadores quanto à proteção de dados na Epagri, como, por exemplo, percentual de usuários treinados, volume de solicitações dos usuários atendidas, número de incidentes reportados, etc.;

● Manter arquivo centralizado no SGP-e contendo registros completos das ações e evidências relacionadas à LGPD.

8.6.3 Departamento Estadual de Gestão da Tecnologia da Informação (DEGTI)

● Apoiar a implementação de controles técnicos de segurança da informação;
● Manter sistemas de proteção atualizados.

8.6.4 Departamento Estadual de Marketing e Comunicação (DEMC):

● Apoiar, coordenar e executar atividades de editoração técnica com fins institucionais, informativos ou educativos, relacionadas ao respectivo Plano;
● Produzir e editar conteúdo jornalístico relacionado à divulgação do respectivo Plano.

8.6.5 Gestores de Contratos e de Projetos

● Assegurar que terceiros estejam em conformidade com a LGPD.

8.6.6 Usuários

● Cumprir as diretrizes deste Plano e reportar imediatamente incidentes ao superior hierárquico e Encarregado de Dados, conforme Plano de Resposta a Incidentes de Segurança;
● Participar dos treinamentos e ações de conscientização, conforme o Plano de Treinamento e Conscientização dos Usuários sobre Segurança da Informação da POSIN.

8.7 Considerações sobre Tecnologias Emergentes e Inteligência Artificial (IA)

Com o avanço de tecnologias emergentes, como Modelos de Linguagem Generativa (LLMs) e outras soluções de Inteligência Artificial (IA), é imprescindível que a Epagri adote práticas proativas para garantir a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e Lei estadual n. 19.450, de 2025. O uso dessas tecnologias, especialmente aquelas que envolvem o tratamento de grandes volumes de dados, pode

implicar riscos relacionados à privacidade, segurança da informação, transparência e minimização de dados.

8.7.1 Impactos e Riscos das Tecnologias Emergentes

● O uso de **LLMs** e outras ferramentas de IA pode envolver os seguintes riscos, especialmente no que tange ao tratamento de dados pessoa

● **Processamento indevido de dados pessoais** em interações com IA, especialmente em ferramentas de uso aberto, como *chatbots* e assistentes virtuais;

● **Risco de reidentificação** a partir de dados anonimizados ou de larga escala, se não houver controle adequado sobre os dados utilizados para treinamento de IA;

● **Armazenamento e uso indevido de dados**, incluindo a geração de respostas baseadas em dados sensíveis fornecidos pelos usuários sem a devida justificativa ou base legal;

● **Impacto no direito à privacidade**, em razão da potencial manipulação de dados pessoais e do uso de dados sem consentimento explícito ou transparência adequada.

8.7.2 Diretrizes para o Uso Responsável de IA e LLMs

● A fim de mitigar os riscos associados ao uso dessas tecnologias, a Epagri adota as seguintes diretrizes:

● **Evitar o uso de dados pessoais ou sensíveis** sem uma base legal adequada em ferramentas baseadas em IA, como LLMs, especialmente quando a origem ou o tratamento desses dados não for controlado ou auditado;

● **Implementar controles internos** rigorosos para garantir que o uso de IA esteja alinhado com a LGPD e com as políticas de segurança da informação e proteção de dados da Epagri;

● **Promover capacitação e conscientização** contínua sobre o uso seguro e ético dessas ferramentas, incluindo treinamentos direcionados aos usuários no desenvolvimento ou no uso dessas tecnologias.

8.7.3 Atribuições do DEGTI e DPO na Implementação de Tecnologias Emergentes

O **DEGTI** e o **Encarregado de Dados Pessoais** são responsáveis por:

● **Garantir que todas as tecnologias emergentes** adotadas pela Epagri sejam avaliadas previamente quanto à conformidade com a LGPD e com as políticas internas de segurança da informação e privacidade;

● **Promover a inclusão de cláusulas de proteção de dados** nos contratos com fornecedores e prestadores de serviços que utilizem IA ou tecnologias emergentes, assegurando a conformidade com a legislação e minimizando riscos para a Epagri.

8.8 Disposições finais

● Este Plano será revisado sempre que houver alteração legislativa relevante ou mudança significativa nos processos da Epagri;

● Casos omissos serão analisados pelo Encarregado de Dados Pessoais, com base na LGPD e nas orientações da ANPD;

● A adoção das medidas previstas neste Plano não exclui a necessidade de observar as demais políticas internas de segurança e gestão de riscos.

9 ANEXO VIII - PLANO DE TREINAMENTO E CONSCIENTIZAÇÃO DOS USUÁRIOS SOBRE SEGURANÇA DA INFORMAÇÃO

9.1 Apresentação

A Epagri, comprometida com o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD), estabelece este Plano como parte integrante da Política de Segurança da Informação (POSIN). Ele visa garantir que todos os usuários compreendam e apliquem boas práticas de segurança da informação, promovendo uma cultura organizacional voltada à proteção de dados e à prevenção de incidentes de segurança.

9.2 Objetivos

Os objetivos deste Plano incluem:

- Proteger dados pessoais e dados pessoais sensíveis tratados pela Epagri;
- Capacitar, por meio de treinamentos contínuos e campanhas de conscientização, os usuários para compreender e aplicar as regras da POSIN e da LGPD;
- Promover a conscientização sobre a importância da proteção de dados pessoais;
- Reduzir riscos e incidentes de segurança por meio da educação continuada e boas práticas;
- Fortalecer a cultura de responsabilidade na proteção de dados pessoais e de dados pessoais sensíveis em todos os níveis da Empresa.

9.3 Campo de Aplicação

Este Plano se aplica a todos os usuários da Epagri, incluindo empregados públicos, terceirizados, estagiários, bolsistas e demais colaboradores que realizem o tratamento de dados pessoais na Empresa.

9.4 Legislação e Boas Práticas

- Lei Federal n º 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- Resolução CD/ANPD nº 18, de 2024 (Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais);

● Decreto estadual nº 1.892, de 2022 (atribuições e requisitos da função de encarregado pelo tratamento de dados pessoais);

● Instrução Normativa SEA nº 20, de 2021 (Política de Segurança da Informação – POSIN);

● ABNT NBR ISO/IEC 27001 (Segurança da informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação).

9.5 Diretrizes Gerais

9.5.1 Métodos dos Treinamentos e Programas de Conscientização dos Usuários

Para o desenvolvimento e a execução dos treinamentos e programas de conscientização, serão utilizados os seguintes métodos:

9.5.1.1 Produção de Conteúdo Multimídia

● Desenvolver vídeos curtos e dinâmicos, com até 2 (dois) minutos de duração, em formatos adequados para redes internas e plataformas digitais, com foco em um único tema por vídeo. O formato, que pode incluir animações, infográficos interativos e narrativas visuais, deve reforçar a retenção da mensagem;

● Expandir o uso do "Minuto Proteção de Dados Pessoais", utilizando ferramentas necessárias para engajamento e avaliação de aprendizado.

9.5.1.2 Materiais Didáticos Interativos

● Criar manuais e guias digitais responsivos, com navegação intuitiva e recursos interativos, como *links* para vídeos explicativos e ferramentas de autoavaliação;

● Desenvolver *e-books* com linguagem acessível e cenários práticos aplicáveis ao cotidiano e contexto da Epagri.

9.5.1.3 Plataforma de *e-Learning*

● Utilizar uma plataforma moderna de aprendizado (*Learning Management System – LMS*) para hospedar cursos *online* modulares, com trilhas de aprendizado personalizadas para diferentes perfis de usuários.

9.5.1.4 Cenários Práticos e Estudos de Caso

● Integrar ao conteúdo estudos de caso reais ou fictícios adaptados à realidade da Epagri, destacando situações críticas e como solucioná-las de forma adequada.

9.5.1.5 Campanhas semestrais ou anuais de Conscientização

● Realizar campanhas temáticas em sinergia com o "Minuto Proteção de Dados Pessoais", abordando tópicos específicos e urgentes, como proteção contra *phishing*, uso seguro de senhas, reportes de incidentes de segurança e boas práticas no trabalho;

● Utilizar os canais de comunicação corporativos para disseminar materiais e reforçar mensagens-chave.

9.5.2 Capacitação em Cascata

Os treinamentos sobre proteção de dados devem ser realizados para os órgãos de governança (Diretoria Executiva e Conselho de Administração) e gerentes das Unidades, garantindo que eles compreendam e difundam a Política de Segurança da Informação da Epagri em suas respectivas áreas de atuação.

Sempre que necessário, os novos dirigentes deverão participar de treinamentos sobre proteção de dados, especialmente em ocasiões como reuniões de dirigentes.

9.5.3 Treinamento sobre Proteção de Dados Pessoais

Os usuários devem realizar um treinamento básico sobre a LGPD para conhecimento sobre direitos, deveres e boas práticas relacionadas à proteção de dados pessoais e ao uso responsável de informações.

Os treinamentos deverão ser periódicos, conforme a necessidade e alterações normativas sobre proteção de dados pessoais.

O Encarregado de Dados deve manter esses treinamentos documentados em processo no Sistema de Gestão de Processos Eletrônicos (SGP-e) para eventuais auditorias da Agência Nacional de Proteção de Dados (ANPD) ou de outros órgãos de controle.

9.5.4 Minuto Proteção de Dados Pessoais

Para reforçar a conscientização de maneira dinâmica e eficaz, será utilizado o recurso já implementado pela Epagri: Minuto Proteção de Dados Pessoais.

Essa série de vídeos curtos, disponibilizada mensalmente ao longo de no mínimo 12 (doze) meses, aborda temas específicos de segurança da informação e proteção de dados. A proposta é oferecer conteúdo de fácil assimilação, garantindo engajamento contínuo dos colaboradores.

9.5.5 Treinamentos Direcionados

Usuários de setores que lidam com grande volume de dados (especialmente dados pessoais sensíveis), participarão de treinamentos específicos e direcionados, alinhados aos riscos e responsabilidades de suas funções, conforme o art. 50 da LGPD. Esses treinamentos visam garantir o cumprimento da LGPD, mitigar riscos e reforçar a segurança da informação.

9.6 Atribuições e Responsabilidades

9.6.1 Diretoria Executiva

- Demonstrar o comprometimento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais, conforme o art. 50, § 2º, inciso I, da LGPD;
- Apoiar e promover a cultura de proteção de dados na Epagri;
- Assegurar a alocação de recursos necessários para a execução deste Plano.

9.6.2 Encarregado de Proteção de Dados (DPO)

- Coordenar, desenvolver e revisar periodicamente este Plano de Treinamento e Conscientização;
- Conduzir treinamentos e orientar os usuários a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Atuar como ponto focal na implementação e monitoramento contínuo do Plano, além de garantir a conformidade com a legislação vigente;
- Apresentar relatórios e informações quanto à adesão dos usuários aos treinamentos e programas de conscientização;
- Documentar os treinamentos realizados.

9.6.3 Departamento Estadual de Gestão da Tecnologia da Informação (DEGTI)

● Implementar medidas técnicas de segurança da informação para proteger dados pessoais;

● Apoiar as atividades de capacitação dos usuários na área de tecnologia da informação e de segurança cibernética;

● Prover ferramentas tecnológicas para suprir a demanda dos treinamentos e a conscientização dos usuários.

9.6.4 Departamento Jurídico (DJUR)

● Apoiar o Encarregado de Dados na resolução de questões jurídicas relacionadas à proteção de dados;

● Prestar consultoria e assessoramento sobre a legislação de proteção de dados pessoais;

● Orientar o Encarregado de Dados e os dirigentes responsáveis pelas Unidades de gestão sobre matéria jurídica envolvendo proteção de dados pessoais;

● Emitir informações e pareceres sobre questões de natureza jurídica envolvendo dados pessoais.

9.6.5 Departamento Estadual de Gestão de Pessoas (DEGP)

● Apoiar programas de capacitação e desenvolvimento contínuos em segurança da informação, proteção de dados e privacidade.

9.6.6 Departamento Estadual de Marketing e Comunicação (DEMC)

● Apoiar, coordenar e executar atividades de editoração técnica com fins institucionais, informativos ou educativos, relacionadas ao respectivo Plano;

● Produzir e editar conteúdo jornalístico relacionado à divulgação do respectivo Plano.

9.6.7 Gestores de Unidades da Epagri

● Promover e fomentar a participação das suas equipes nos treinamentos sobre proteção de dados pessoais;

● Reforçar o cumprimento das diretrizes sobre proteção de dados pessoais nas unidades sob sua gestão.

9.6.8 Usuários

● Participar dos treinamentos e programas de conscientização, aplicando as boas práticas aprendidas;

● Reportar incidentes de segurança imediatamente ao superior hierárquico e Encarregado de Dados, conforme o Plano de Resposta a Incidentes de Segurança.

9.7 Monitoramento e Avaliação

Para assegurar a eficácia deste Plano, serão adotadas a s seguintes ações de monitoramento e avaliação:

● Utilizar ferramentas analíticas e indicadores para medir a adesão e os resultados dos treinamentos, como índices de participação, percentual de usuários treinados, pontuações em testes e retorno dos usuários;

● Realizar pesquisas de satisfação para aprimorar os conteúdos futuros, de acordo com as necessidades e sugestões dos usuários;

● Apresentar relatórios periódicos à Diretoria Executiva.

9.8. Disposições finais

Este Plano entra em vigor na data de sua aprovação pela Diretoria Executiva da Epagri e deve ser revisado sempre que houver necessidade de adequação às necessidades da Empresa, adaptação a novas tecnologias, atendimento a requisitos legais e mudanças nos processos internos.

As revisões deste Plano serão conduzidas pelo Encarregado de Dados.

GLOSSÁRIO

Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique.

Ameaça: para os fins deste Plano, o conjunto de fatores com o potencial de causar um incidente de segurança da informação que pode resultar em danos a um sistema ou prejuízos à Epagri. É um risco com consequência negativa para a Epagri.

Análise de vulnerabilidades: verificação e exame técnico de vulnerabilidades para determinar onde elas estão localizadas e como foram exploradas.

ANPD: Agência Nacional de Proteção de Dados, autarquia federal responsável por fiscalizar e regulamentar o uso de dados pessoais no Brasil, promovendo a proteção da privacidade e o cumprimento da LGPD. Suas atribuições incluem elaborar diretrizes, aplicar sanções, esclarecer dúvidas, promover a conscientização pública e cooperar com outras agências em questões relacionadas a dados pessoais. Ressalta-se que a Medida Provisória n. 1.317, de 17 de setembro de 2025 transformou a Autoridade Nacional de Proteção de Dados em Agência Nacional de Proteção de Dados.

Apetite a risco: nível de risco (impacto x probabilidade) que a Epagri está disposta a aceitar.

Ativos de informação: são dados em tráfego ou armazenados em sistemas de informação em formato digital (elétrico, magnético ou óptico) ou físico (impressos), incluindo qualquer meio de armazenamento, transmissão e processamento desses dados, como equipamentos, sistemas e locais onde se encontram esses meios. Exemplo: documentos, base de dados, contratos, documentação de sistemas, procedimentos, manuais, *logs* de sistemas, planos, guias, programas de computador (*softwares)*, servidores, computadores, *switches*, *storages*, e-mails, arquivos pessoais e compartilhados, bancos de dados e conteúdo da *web* específicos.

Ativos físicos: equipamentos que compõem os recursos de tecnologia e de informática, como computadores, mídias removíveis, equipamentos de comunicação e conectividade, entre outros, e suas respectivas instalações.

Ativos de *softwares*: programas, sistemas, ferramentas e utilitários adquiridos, licenciados ou desenvolvidos pela Epagri e que fazem parte das atividades dos usuários em seu dia a dia. Ex.: SAFI, SEPLAN, GMail, Google Drive, Banco de Dados *Oracle* etc.

Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

Banco de dados: conjunto estruturado de dados, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Classificação de sigilo de informação: é o procedimento realizado pela CIAI que define o grau de sigilo de informações listadas no art. 23 da LAI e art. 27 do Decreto estadual nº 1.048, de 2012.

Confidencialidade: propriedade pela qual se assegura que o dado pessoal ou sigiloso não esteja disponível ou não seja revelado a pessoas, empresas, sistemas, órgãos ou entidades não autorizados. A Epagri adota a publicidade como regra geral e o sigilo como exceção apenas nos casos previstos na legislação.

Consequência: resultado de um evento que afeta os objetivos. Uma consequência pode ser certa ou incerta e pode ter efeitos positivos ou negativos sobre os objetivos.

Conta administrativa: *login* de acesso aos recursos de tecnologia da informação com privilégios de cadastro, manutenções e exclusões.

Conta nomeada: *login* de acesso aos recursos de tecnologia da informação disponibilizado pela Epagri aos usuários.

Conta corporativa: *login* de acesso aos recursos de tecnologia da informação disponibilizado para unidades da Epagri ou atividades que necessitem de conta específica que não a conta nomeada.

Conta de serviço: *login* de acesso aos recursos de tecnologia da informação necessária a um procedimento automático (aplicação, *script*, entre outros). Um exemplo é o *login* utilizado para enviar mensagens de renovação de senha.

Continuidade de Negócios: capacidade da Epagri de continuar a entrega de seus produtos ou serviços em um nível aceitável, bem como funções essenciais, durante e após um evento disruptivo.

Controlador: no contexto de proteção de dados pessoais, é pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No ambiente Epagri, o controlador é a própria Epagri, que exigirá das pessoas físicas e jurídicas, com quem se relacione, o cumprimento da LGPD e de suas políticas, nas situações que envolvam o tratamento de dados pessoais originários da Epagri. Os empregados da Epagri, quando a Empresa atua como controladora de dados pessoais, não são considerados operadores; eles agem em nome da própria Epagri.

Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Disponibilidade: propriedade pela qual se assegura que o dado esteja acessível e utilizável, sob demanda, por uma pessoa natural ou determinado sistema, órgão ou entidade devidamente autorizados.

Documento: unidade de registro de informações, qualquer que seja o suporte ou formato.

***E-books*:** abreviação de "eletronic book", ou seja, livro eletrônico. É uma cópia digital de um livro, panfleto, brochura ou guia que pode ser lido em dispositivos eletrônicos.

Encarregado de Dados (DPO): pessoa indicada pelo controlador para atuar como canal de comunicação com os titulares e a ANPD.

Evento Disruptivo: qualquer incidente que possa interromper parcial ou totalmente as atividades e a entrega de produtos e serviços da Epagri, prejudicando o atingimento dos objetivos institucionais.

Gamificação: aplicação de elementos de jogos em contextos não relacionados a jogos, com o objetivo de motivar e ensinar. No treinamento corporativo pode ser usada para desenvolver habilidades específicas dos funcionários, praticar e dominar tarefas específicas.

Gestão de mudanças nos aspectos relativos à segurança da informação: processo estruturado que visa aumentar a probabilidade de sucesso em mudanças, com mínimos impactos, e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

Gestão de riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações para fornecer razoável certeza quanto ao alcance dos objetivos da Epagri.

Gestor do ativo de informação: usuário responsável pela administração do ativo, seja digital ou físico.

IA: Inteligência Artificial é um conjunto de tecnologias que permitem aos computadores executar uma variedade de funções avançadas, incluindo a capacidade de ver, entender e traduzir idiomas falados e escritos, analisar dados, fazer recomendações e muito mais.

Identificação de riscos: processo de busca, reconhecimento e descrição de riscos.

Incerteza: incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros.

Incidente de segurança: qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados, sejam pessoais ou não.

Incidente de segurança que possa acarretar risco ou dano relevante: é aquele que pode afetar significativamente interesses e direitos fundamentais dos titulares de dados pessoais e, cumulativamente, envolver, pelo menos, um dos seguintes critérios: I - dados pessoais sensíveis; II - dados de crianças, de adolescentes ou de idosos; III - dados financeiros; IV - dados de autenticação em sistemas; V - dados protegidos por sigilo legal, judicial ou profissional; ou VI - dados em larga escala.

Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

Informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

Informação pessoal: aquela relacionada à pessoa física identificada ou identificável. Inclui dados pessoais e dados pessoais sensíveis.

Inventário de dados: documento que descreve o ciclo de vida dos dados pessoais tratados pela organização.

Integridade: no contexto deste Plano, é a propriedade pela qual se assegura que o dado não foi modificado ou destruído de maneira não autorizada ou acidental.

LGPD: Lei Geral de Proteção de Dados Pessoais.

LLM: *Large Language Models* significa Grandes Modelos de Linguagem, são sistemas de inteligência artificial treinados com grandes volumes de dados textuais com o objetivo de compreender, processar e gerar linguagem natural.

***Log* (Registro de Auditoria):** registro de eventos relevantes em um dispositivo ou sistema computacional.

Matriz de risco: instrumento que auxilia a classificação dos riscos em aceitáveis, gerenciáveis, indesejáveis e inaceitáveis, em função das escalas de impacto e probabilidade. A escala de impacto mede o impacto de determinado risco nos objetivos. A escala de probabilidade mede a frequência que um risco pode ocorrer em determinado intervalo de tempo.

MFA: sigla de autenticação de multifatores (*multifactor authentication*). É um processo de login de conta com várias etapas que obriga o usuário a inserir informações que vão além de uma simples senha.

Modelo das Três Linhas do IIA: é um modelo de organizar funções dentro de uma organização para garantir uma boa governança e gestão de riscos. O modelo ajuda a proteger e criar valor, garantindo que todos saibam suas funções e trabalhem juntos de forma coordenada.

Nível de risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências (impactos) e de suas probabilidades.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. P. ex.: a Epagri detém dados pessoais de seus empregados, ao formalizar um contrato com uma empresa para o Sistema de Registro Eletrônico de Ponto (SREP), essa empresa contratada será o operador, e deverá cuidar desses dados recebidos seguindo as ordens da Epagri (controlador) e as regras da LGPD.

***Phishing*:** é um tipo de crime cibernético que tem como objetivo roubar informações pessoais ou acessar contas *on-line*. Os criminosos usam mensagens enganosas, como e-mails, mensagens de texto ou anúncios, para convencer as vítimas a revelarem informações confidenciais.

Plano de Contingência: conjunto de ações para lidar com situações inesperadas e reduzir prejuízos.

Probabilidade: chance de algo acontecer.

Rede de computadores: conjunto de equipamentos de rede, estações de trabalho e demais equipamentos interligados com o objetivo de disponibilizar serviços de TI aos usuários das Unidades que compõem a Epagri.

Resiliência Organizacional: capacidade da instituição de resistir, adaptar-se e se recuperar de adversidades e de eventos disruptivos.

Responsável pela informática: usuário responsável pelo suporte de informática nas Unidades/região ou, na ausência deste, o Departamento Estadual de Gestão da Tecnologia da Informação (DEGTI).

Responsável pela rede Epagri: usuário responsável pela manutenção e operação dos serviços e servidores de rede, como *e-mail*, *web*, aplicativos em geral.

Responsável pelas unidades da Epagri: gestor da unidade e ou das unidades hierarquicamente subordinadas, conforme o Regimento Interno da Epagri e plano gerencial.

Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. É o efeito da incerteza nos objetivos. Esse efeito é um desvio em relação ao esperado, que pode ser positivo (oportunidades), negativo (ameaças) ou ambos (ABNT NBR ISO 31000:2018 e 37000:2022). O risco é medido em termos de impacto e de probabilidade.

Risco de segurança da informação: risco associado a uma ou mais vulnerabilidades em ativos de informação. Pode resultar em impactos negativos para a Epagri (ameaças) e afetar as suas operações, conformidade, estratégia ou situação orçamentária e financeira.

Sistema Crítico: sistema ou processo cuja paralisação afeta significativamente a missão institucional da organização.

Sistemas de informação corporativos: são aqueles destinados a atender os processos operacionais da Empresa, sejam eles de negócio (pesquisa, extensão, etc.), de apoio (financeiros, administrativos, pessoal, etc.) ou de gestão (permitem a visualização e análise de resultados da Empresa), conforme a cadeia de valor da Epagri. Incluem programas de computador, aplicativos (*apps*) etc.

Teste de invasão: metodologia para testar a eficácia e a resiliência de ativos através da identificação e exploração de fraquezas nos controles de segurança e da simulação das ações e objetivos de um atacante, como, por exemplo, *hacker*, *sites* maliciosos etc.

Terceiros: pessoas jurídicas ou físicas que não integram a Epagri. Incluem operadores e outras pessoas com quem a Epagri se relaciona externamente.

Titular: pessoa natural a quem se referem os dados pessoais.

Tratamento: toda operação realizada com dados pessoais ou sigilosos, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Tratamento de riscos: conjunto de procedimentos, ações ou medidas que visam evitar, mitigar, transferir ou aceitar o risco, conforme o apetite a risco.

Treinamento Simulado: exercício prático para preparar a equipe frente a um possível incidente.

Unidades da Epagri: consideram-se como Unidades da Epagri os Órgãos de Direção Superior, as Unidades e Comitês de Assessoramento Superior, Departamentos Estaduais e Unidades Descentralizadas, na forma do Regimento Interno.

Usuário: empregado público, estagiário, bolsista, aprendiz, empregado ou servidor público à disposição de outras instituições, empregado ou servidor público cedido por outras instituições, prestadores de serviço voluntário, terceirizados, instrutores, alunos e demais colaboradores que estão autorizados a utilizar a rede, os equipamentos de informática e os sistemas de informação das Unidades da Epagri.

Vulnerabilidade: deficiências existentes em tecnologias, sistemas, ambientes, pessoas ou nos próprios processos da Epagri que podem levar a um evento com um impacto para a Epagri. A causa de um risco é a soma de uma fonte e de uma vulnerabilidade (causa = fonte + vulnerabilidade).

www.epagri.sc.gov.br
www.youtube.com/epagritv
www.facebook.com/epagri
www.instagram.com/epagri
linkedin.com/company/epagri
http://publicacoes.epagri.sc.gov.br
www.x.com/EpagriOficial